Bitdefender

GravityZone

ADMINISTRATORHANDBUCH

Bitdefender GravityZone
Administratorhandbuch

Veröffentlicht 2015.09.09

Copyright© 2015 Bitdefender

Rechtlicher Hinweis

Alle Rechte vorbehalten. Bestandteile dieses Handbuches dürfen weder in elektronischer noch mechanischer Form reproduziert werden. Dies gilt auch für das Fotokopieren, Aufnehmen oder jegliche andere Form von Datenspeicherung oder Informationsbeschaffung, ohne die Zustimmung von Bitdefender. Ausnahmen gelten für Zitate in Verbindung mit Testberichten. Der Inhalt darf in keiner Weise verändert werden.

Warnung und Haftungsausschluss. Dieses Produkt und die dazugehörige Dokumentation sind urheberrechtlich geschützt. Die Informationen in diesem Dokument werden „ohne Mängelgewähr" gegeben. Obwohl dieses Dokument mit äußerster Sorgfalt erstellt und geprüft wurde, übernehmen die Autoren keinerlei Haftung für tatsächlich oder angeblich auftretende Schäden bzw. Datenverluste, die direkt oder indirekt durch die Informationen in diesem Dokumente entstehen könnten oder bereits entstanden sind.

Dieses Handbuch enthält Verweise auf andere, nicht von Bitdefender erstellte Webseiten, die auch nicht von Bitdefender kontrolliert werden, somit übernimmt Bitdefender auch keine Verantwortung in jeglicher Art für den Inhalt dieser Webseiten. Der Besuch der in diesem Dokument aufgelisteten Drittanbieter-Webseiten erfolgt damit auf eigene Gefahr. Bitdefender stellt diese Links der Einfachheit zur Verfügung. Dies bedeutet nicht, dass Bitdefender den Inhalt einer Website Dritter befürwortet oder Verantwortung dafür übernimmt.

Warenzeichen. Es erscheinen eingetragene Warenzeichen in diesem Dokument. Alle eingetragenen und nicht eingetragenen Warenzeichen in diesem Dokument sind das alleinige Eigentum der jeweiligen Besitzer.

Bitdefender

Inhaltsverzeichnis

Vorwort vi
1. Konventionen in diesem Handbuch vi
1. Über GravityZone 1
1.1. GravityZone-Sicherheitsdienste 1
1.2. GravityZone-Architektur 2
1.2.1. Web-Konsole (Control Center) 2
1.2.2. Sicherheitsagenten 2
2. Erste Schritte 8
2.1. Verbinden mit dem Control Center 8
2.2. Control Center auf einen Blick 9
2.2.1. Übersicht über die Control Center 9
2.2.2. Tabellendaten 11
2.2.3. Symbolleisten 12
2.2.4. Kontextmenü 12
2.3. Verwalten Ihres Kontos 13
2.4. Ändere Login Passwort 14
2.5. Ihr Unternehmen verwalten 14
3. Benutzerkonten verwalten 17
3.1. Benutzerrollen 19
3.2. Benutzerrechte 20
3.3. Benutzerkonten erstellen 21
3.4. Konten bearbeiten 22
3.5. Benutzerkonten löschen 23
3.6. Anmeldepasswörter zurücksetzen 23
4. Endpunkte verwalten 24
4.1. Status der Endpunkts überprüfen 26
4.1.1. Endpunktverwaltungsstatus 26
4.1.2. Endpunktverbindungsstatus 26
4.1.3. Endpunktsicherheitsstatus 28
4.2. Endpunktdetails anzeigen 29
4.3. Endpunkte in Gruppen organisieren 33
4.4. Sortieren, Filtern und Suchen von Endpunkten 34
4.4.1. Endpunkte sortieren 35
4.4.2. Endpunkte filtern 35
4.4.3. Nach Endpunkten suchen 38
4.5. Aufgaben ausführen 38
4.5.1. Scan 39
4.5.2. Installieren 48
4.5.3. Client Deinstallieren 52
4.5.4. Client aktualisieren 53
4.5.5. Client neu konfigurieren 53
4.5.6. Client neu starten 55
4.5.7. Netzwerkerkennung 55

4.6. Schnellberichte erstellen . . . 56
4.7. Richtlinien zuweisen . . . 56
4.8. Endpunkte aus dem Netzwerkinventar löschen . . . 58
4.9. Aufgaben anzeigen und verwalten . . . 59
4.9.1. Aufgabenstatus überprüfen . . . 59
4.9.2. Aufgabenberichte anzeigen . . . 61
4.9.3. Erneutes Ausführen von Aufgaben . . . 61
4.9.4. Aufgaben löschen . . . 62
4.10. Zugangsdaten-Manager . . . 62
4.10.1. Zugangsdaten zum Zugangsdaten-Manager hinzufügen . . . 63
4.10.2. Zugangsdaten aus dem Zugangsdaten-Manager löschen . . . 64
5. Sicherheitsrichtlinien . . . 65
5.1. Policies verwalten . . . 67
5.1.1. Richtlinien erstellen . . . 67
5.1.2. Richtlinieneinstellungen ändern . . . 68
5.1.3. Richtlinien umbenennen . . . 69
5.1.4. Richtlinien löschen . . . 69
5.1.5. Netzwerkobjekten Richtlinien zuweisen . . . 70
5.2. Richtlinien für Computer und virtuelle Maschinen . . . 72
5.2.1. Allgemein . . . 73
5.2.2. Malware-Schutz . . . 84
5.2.3. Firewall . . . 104
5.2.4. Inhalts -Steuer. . . . 116
5.2.5. Gerätesteuerung . . . 128
5.2.6. Relais . . . 132
6. Überwachungs-Dashboard . . . 135
6.1. Portlet-Daten neu laden . . . 136
6.2. Portlet-Einstellungen bearbeiten . . . 136
6.3. Ein neues Portlet hinzufügen . . . 136
6.4. Ein Portlet entfernen . . . 137
6.5. Portlets neu anordnen . . . 137
7. Berichte verwenden . . . 139
7.1. Verfügbare Berichtstypen . . . 140
7.2. Berichte erstellen . . . 144
7.3. Geplante Berichte anzeigen und verwalten . . . 146
7.3.1. Berichte betrachten . . . 147
7.3.2. Geplante Berichte bearbeiten . . . 148
7.3.3. Geplante Berichte löschen . . . 150
7.4. Berichtbasierte Aktionen ausführen . . . 150
7.5. Berichte speichern . . . 151
7.5.1. Berichte exportieren . . . 151
7.5.2. Berichte herunterladen . . . 151
7.6. Berichte per E-Mail versenden . . . 152
7.7. Berichte ausdrucken . . . 152
8. Quarantäne . . . 153
8.1. Die Quarantäne im Detail . . . 153

8.2. Quarantäne für Computer und virtuelle Maschinen ... 155
8.2.1. Quarantäne-Details anzeigen ... 155
8.2.2. Verwalten von Dateien in der Quarantäne ... 155
9. Benutzeraktivitätsprotokoll ... 158
10. Benachrichtigungen ... 160
10.1. Benachrichtigungsarten ... 160
10.2. Benachrichtigungen anzeigen ... 162
10.3. Benachrichtigungen löschen ... 163
10.4. Benachrichtigungseinstellungen konfigurieren ... 163
11. Hilfe erhalten ... 166
11.1. Bitdefender-Support-Center ... 166
11.2. Hilfe anfordern ... 167
11.3. Verwenden des Support-Tools ... 168
11.3.1. Das Support-Tool unter Windows verwenden ... 168
11.3.2. Das Support-Tool unter Linux ... 169
11.4. Kontaktinformation ... 171
11.4.1. Internet-Adressen ... 171
11.4.2. Händler vor Ort ... 171
11.4.3. Bitdefender-Niederlassungen ... 172
A. Anhänge ... 175
A.1. Netzwerkobjekttypen und -status ... 175
A.1.1. Netzwerkobjekttypen ... 175
A.1.2. Netzwerkobjektstatus ... 175
A.2. Anwendungsdateitypen ... 176
A.3. Systemvariablen ... 177
Glossar ... 179

Vorwort

Dieses Handbuch richtet sich an Netzwerkadministratoren, die mit der Verwaltung von GravityZone innerhalb ihres Unternehmens betraut sind.

In diesem Dokument wird beschrieben, wie Sie mit dem GravityZone Control Center Sicherheitseinstellungen auf Endpunkten unter Ihrem Konto anzeigen und konfigurieren können. Hier erfahren Sie, wie Sie Ihr Netzwerkinventar im Control Center anzeigen, Richtlinien erstellen und auf verwalteten Endpunkten anwenden, Berichte erstellen, Objekte in der Quarantäne verwalten und das Dashboard nutzen.

1. Konventionen in diesem Handbuch

Typografie

In diesem Handbuch werden verschiedene Schriftarten verwendet, um die Lektüre zu erleichtern. In der unten stehenden Tabelle erfahren Sie, was welche Schriftart bedeutet.

Erscheinungsbild	Beschreibung
`Beispiel`	Einzugebende Befehle und Syntaxen, Pfade und Dateinamen, Konfigurationen, Dateiausgaben und andere Eingabetexte sind in `nicht-proportionaler` Schrift gedruckt.
http://www.bitdefender.com	Verweise (Links) auf externe Inhalte wie z.B. Web-Seiten oder FTP-Server.
documentation@bitdefender.com	Verweise auf E-Mail-Adressen, z.B. zur Kontaktaufnahme.
„Vorwort“ (S. vi)	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
Option	Alle Produktoptionen werden **fett gedruckt** dargestellt.
Stichwort	Optionen der Benutzeroberfläche, Stichwörter oder Tastenkombinationen werden durch **Fettdruck** hervorgehoben.

Symbole

Bei diesen Symbolen handelt es sich um Hinweise innerhalb des Textflusses welche mit einer kleinen Grafik markiert sind. Hierbei handelt es sich um Informationen die Sie in jedem Fall beachten sollten.

Beachten Sie

Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.

Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden signifikante Informationen zum jeweiligen Thema bereitgestellt. Es wird nicht empfohlen diese zu übergehen.

Warnung

Diese kritische Information sollten Sie mit höchster Aufmerksamkeit verfolgen. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie sollten diese Informationen sorgsam lesen und verstanden haben, da es sich um eine höchst prekäre Thematik handelt.

1. ÜBER GRAVITYZONE

GravityZone ist eine Sicherheitslösung für Unternehmen, die speziell auf virtuelle und Cloud-Umgebungen zugeschnitten ist, und bietet Sicherheitsdienste für physische Endpunkte und virtuelle Maschinen in der Private und der Public Cloud.

GravityZone ist ein umfassendes Produkt mit einer zentralen Verwaltungskonsole, die entweder von Bitdefender in der Cloud gehostet oder als virtuelle Appliance innerhalb des Unternehmens installiert wird. Über diese Konsole können von zentraler Stelle aus Sicherheitsrichtlinien für eine beliebige Zahl an Endpunkten erstellt, zugewiesen und verwaltet werden, unabhängig vom Typ und geographischen Ort dieser Endpunkte.

GravityZone bietet mehrschichtige Sicherheit für Endpunkte: Viren- und Malware-Schutz mit Verhaltens-Scans, Schutz vor Zero-Day-Attacken, Anwendungssteuerung und Sandbox, Firewall, Geräte- und Inhaltssteuerung.

1.1. GravityZone-Sicherheitsdienste

GravityZone enthält die folgenden Sicherheitsdienste:

- Security for Endpoints
- Security for Virtualized Environments

Security for Endpoints

Die Lösung bietet unauffälligen Schutz für Windows-Desktops, -Laptops und -Servern und setzt dabei auf vielfach ausgezeichnete Malware-Schutz-Technologien kombiniert mit einer Zwei-Wege-Firewall, Angriffserkennung, der Steuerung und Filterung des Internet-Zugriffs, dem Schutz von sensiblen Daten sowie Geräte- und Anwendungssteuerung. Geringer Ressourcenverbrauch bringt Leistungsgewinne. Die Lösung bietet viele Vorteile gegenüber herkömmlicher Malware-Schutz-Software, da sie vielfach ausgezeichnete Sicherheitstechnologien mit hoher Benutzerfreundlichkeit und zentraler Verwaltung über das GravityZone Control Center bietet. Proaktive Heuristiken werden eingesetzt, um bösartige Prozesse aufgrund ihres Verhaltens zu erkennen. Dadurch können neue Bedrohungen in Echtzeit erkannt werden.

Security for Virtualized Environments

Security for Virtualized Environments ist die erste umfassende Sicherheitslösung für virtualisierte Rechenzentren zum Schutz von virtualisierten Servern und Arbeitsplatzrechnern auf Windows- und Linux-Systemen. Die Lösung setzt topmoderne Cache-Technologie ein, die gegenüber herkömmlicher Sicherheitssoftware Gewinne in puncto Leistung und Server-Konsolidierung von bis zu 30 % bringt.

1.2. GravityZone-Architektur

GravityZone besteht aus den folgenden Komponenten:

- Web-Konsole (Control Center)
- Sicherheitsagenten

1.2.1. Web-Konsole (Control Center)

Bitdefender-Sicherheitslösungen werden innerhalb der GravityZone von einer zentralen Stelle aus verwaltet: dem Control Center. Diese Web-Konsole erleichtert die Verwaltung, indem sie einen Überblick über die gesamte Sicherheitslage des Unternehmens bietet und die Steuerung aller Sicherheitsmodule für virtuelle und physische Arbeitsplatzrechner und Server ermöglicht. Dank der Gravity-Architektur ist Control Center in der Lage, die Anforderungen selbst der größten Unternehmen zu erfüllen.

Das Control Center, eine Web-basiserte Oberfläche, lässt sich mit bestehenden System- und Überwachungssystemen integrieren und macht es so sehr leicht, nicht-verwaltete Arbeitsplatzrechner und Server zu schützen.

1.2.2. Sicherheitsagenten

Um Ihr Netzwerk mit Bitdefender zu schützen, müssen Sie die entsprechenden GravityZone-Sicherheitsagenten auf Endpunkten im Netzwerk installieren.

- Bitdefender Endpoint Security Tools
- Endpoint Security for Mac

Bitdefender Endpoint Security Tools

GravityZone schützt physische und virtuelle Maschinen mit Bitdefender Endpoint Security Tools, einem intelligenten Sicherheitsagenten, der sich an die jeweilige Umgebung anpasst und je nach Endpunkttyp automatisch selbst konfiguriert.

Bitdefender Endpoint Security Tools kann auf jeder beliebigen Maschine, egal ob virtuell oder physisch, installiert werden und bietet ein flexibles Scan-System. Das macht die Software zur idealen Wahl für gemischte Umgebungen (mit physischen, virtuellen und Cloud-Elementen).

Bitdefender Endpoint Security Tools benötigt nur eine einzige Richtlinienvorlage für physische und virtuelle Maschinen und nur ein einziges Installationskit für physische und virtuelle Umgebungen. Bitdefender Endpoint Security Tools ist auch mit physischen Linux-Endpunkten (Arbeitsplatzrechnern und Servern) kompatibel.

Scan-Engines

Die Scan-Engines werden während der Bitdefender Endpoint Security Tools-Paketerstellung automatisch festgelegt. Der Endpunkt-Agent erkennt dabei die Konfiguration der Maschine und passt die Scan-Technologie entsprechend an. Administratoren können die Scan-Engines auch manuell anpassen. Dabei können sie unter den folgenden Optionen wählen:

1. **Lokaler Scan**: für Scans, die auf lokalen Endpunkten durchgeführt werden. Der lokale Scan-Modus eignet sich für leistungsstarke Maschinen, auf denen alle Signaturen und Engines gespeichert sind.
2. **Hybrid-Scan mit leichten Engines (Public Cloud)**: mittlerer Ressourcenverbrauch; gescannt wird in der Cloud und zum Teil auch mithilfe lokaler Signaturen. Dieser Scan-Modus reduziert den Ressourcenverbrauch durch Auslagerung der Scan-Aktivität.
3. **Zentralisierter Scan in der Private Cloud**: geringer Ressourcenverbrauch; benötigt einen Security Server zum Scan. In diesem Fall werden keine Signaturen lokal gespeichert. Die Scan-Aktivität wird auf den Security Server ausgelagert.
4. **Zentralisierter Scan (Scan in der Private Cloud mit Security Server) mit Ausweichmöglichkeit* auf lokalen Scan (Volle Engines)**
5. **Zentralisierter Scan (Scan in der Private Cloud mit Security Server) mit Ausweichmöglichkeit* auf Hybrid-Scan (Public Cloud mit leichten Engines)**

Sicherheitsmodule

Bitdefender Endpoint Security Tools enthält die folgenden Sicherheitsmodule:

- Malware-Schutz
- Active Virus Control
- Firewall
- Inhalts -Steuer.
- Gerätesteuerung

- Power -User

Malware-Schutz

Das Malware-Schutzmodul setzt Signatur-Scans und heuristische Analysen (B-HAVE) ein, um Sicherheit vor Viren, Würmern, Trojanern, Spyware, Adware, Keyloggern, Rootkits und anderen Arten bösartiger Software zu bieten.

Bitdefenders Technologie zur Erkennung von Malware umfasst die folgenden Sicherheitsschichten:

- Zunächst kommt eine herkömmliche Scan-Methode zum Einsatz, bei der die überprüften Inhalte mit der Signaturdatenbank abgeglichen werden. Die Signaturdatenbank enthält die Byte-Folgen, die für bekannte Bedrohungen spezifisch sind, und wird von Bitdefender regelmäßig aktualisiert. Diese Scan-Methode erkennt bestätigte Bedrohung, die bereits erforscht und dokumentiert wurden, sehr effektiv. Doch auch wenn die Signaturdatenbank immer umgehend aktualisiert wird, gibt es zwischen der Entdeckung der Bedrohung und der Problemlösung immer ein Zeitfenster, in dem das System eine Schwachstelle hat
- Neue, bisher noch nicht dokumentierte Bedrohungen werden in einer zweiten Schutzebene aufgefangen. Dabei handelt es sich um **B-HAVE**, die heuristische Engine von Bitdefender. Heuristische Algorithmen erkennen Malware anhand bestimmter Verhaltensweisen. B-HAVE führt mutmaßliche Malware in einer virtuellen Umgebung aus, um die Auswirkungen auf das System zu untersuchen und eine Bedrohung auszuschließen. Sollte eine Bedrohung erkannt werden, wird eine Ausführung des Programms verhindert.

Active Virus Control

Für Bedrohungen, die selbst von der heuristische Engine nicht erkannt werden, wurde mit Active Virus Control (AVC) eine dritte Schutzebene eingerichtet.

Active Virus Control überwacht ununterbrochen die laufenden Prozesse und bewertet verdächtige Verhaltensweisen wie zum Beispiel das Verbergen des Prozesstyps, die Ausführung von Code im Adressraum eines anderen Prozesses (Übernahme des Prozessspeichers zur Erweiterung von Rechten), Replikationsversuche, das Ablegen von Dateien, das Verbergen vor Anwendungen zur Prozessübersicht usw. Jedes verdächtige Verhalten steigert den Verdachtswert des Prozesses. Sobald ein Schwellenwert überschritten wird, wird ein Alarm ausgelöst.

Wichtig
Dieses Modul besteht nur für unterstützte Windows-Desktop- und -Server-Betriebssysteme zur Verfügung.

Firewall

Die Firewall steuert den Zugriff von Anwendungen auf das Netzwerk sowie auf das Internet. Eine umfangreiche Datenbank enthält eine Liste bekannter, vertrauenswürdiger Anwendungen, denen automatisch Zugriff gewährt wird. Zudem kann die Firewall das System vor Port-Scans schützen, die gemeinsame Nutzung der Internet-Verbindung (ICS) beschränken und Benachrichtigungen generieren, sobald neue Knoten mit dem Drahtlosnetzwerk verbunden werden.

Wichtig
Dieses Modul steht nur für Windows-Arbeitsplätze zur Verfügung.

Inhalts -Steuer.

Mit dem Modul Inhaltssteuerung können Unternehmensrichtlinien für zugelassenen Datenverkehr, Internetzugriff, Datenschutz und Anwendungssteuerung durchgesetzt werden. Administratoren können Scan-Optionen und -Ausschlüsse für den Datenverkehr festlegen, den Internetzugriff auf bestimmte Zeiten beschränken, einzelne Internetkategorien oder URLs blockieren, Identitätsschutzregeln konfigurieren und Rechte für die Verwendung bestimmter Anwendungen festlegen.

Wichtig
Dieses Modul steht nur für Windows-Arbeitsplätze zur Verfügung.

Gerätesteuerung

Mit dem Modul Gerätesteuerung kann mithilfe von in Richtlinien festgelegten Blockier-Regeln und Ausnahmen verhindert werden, dass sensible Daten unbefugt weitergegeben werden und Infektionen über externe Datenträger ins Netzwerk gelangen. Dies ist für eine große Bandbreite an Gerätearten möglich wie zum Beispiel USB-Sticks, Bluetooth-Geräte, CD/DVD-Player, Speichermedien und vieles mehr.

Wichtig
Dieses Modul besteht nur für unterstützte Windows-Desktop- und -Server-Betriebssysteme zur Verfügung.

Power -User

Control-Center-Administratoren können über Richtlinieneinstellungen bestimmten Endpunkt-Benutzern Power-User-Rechte gewähren. Mit dem Power-User-Modul können Benutzern Administratorrechte verliehen werden, mit denen sie über die lokale Konsole Sicherheitseinstellungen anzeigen und verändern können. Im Control Center wird eine Benachrichtigung angezeigt, wenn ein Endpunkt sich im Power-User-Modus befindet, und Control Center-Administratoren können lokale Sicherheitseinstellungen immer außer Kraft setzen.

Wichtig
Dieses Modul besteht nur für unterstützte Windows-Desktop- und -Server-Betriebssysteme zur Verfügung.

Endpunktrollen

Relais-Rolle

Endpunktagenten mit der Rolle Bitdefender Endpoint Security Tools Relay fungieren als Kommunikations- Proxy- und Update-Server für andere Endpunkte im Netzwerk. Endpunkt-Agenten mit Relais-Rolle werden besonders in Unternehmen mit isolierten Netzwerken benötigt, in denen sämtlicher Datenverkehr über einen einzelnen Zugangspunkt läuft.

In Unternehmen mit großen, geographisch dezentralen Netzwerken reduzieren Relais-Agenten die benötigte Bandbreite, indem sie verhindern, dass geschützte Endpunkte eine direkte Verbindung zur GravityZone herstellen.

Nachdem ein Bitdefender Endpoint Security Tools Relay im Netzwerk installiert wurde, können andere Endpunkte per Richtlinie so konfiguriert werden, dass sie über den Relais-Agenten mit dem Control Center kommunizieren.

Bitdefender Endpoint Security Tools Relay-Agenten haben die folgenden Funktionen:

- Alle ungeschützten Endpunkte im Netzwerk finden.

  Diese Funktion ist für die sichere Agenteninstallation in einer GravityZone-Cloud-Umgebung unabdingbar.
- Den Endpunkt-Agenten im lokalen Netzwerk installieren.
- Geschützte Endpunkte im Netzwerk auf dem neuesten Stand halten.
- Die Kommunikation zwischen dem Control Center und verbundenen Endpunkten gewährleisten.

- Als Proxy-Server für geschützte Endpunkte fungieren.
- Optimierung des Netzwerkverkehrs während Updates, Installationen, Scan-Vorgänge und andere ressourcenintensive Aufgaben ausgeführt werden.

Wichtig
Diese Rolle steht nur für unterstützte Windows-Desktop- und -Server-Betriebssysteme zur Verfügung.

Endpoint Security for Mac

Endpoint Security for Mac ist ein leistungsstarker Virenscanner, der sämtliche Arten von Malware aufspüren und entfernen kann: Viren, Spyware, Trojaner, Keylogger, Würmer und Adware. Das Programm ist auf Intel-basierte Macintosh-Arbeitsplatzrechner und -Laptops ausgelegt, auf denen Mac OS X ab Version 10.7 läuft.

Endpoint Security for Mac enthält nur das Malware-Schutz-Modul; die verfügbare Scan-Technologie ist **Lokaler Scan**; alle Signaturen und Engines werden lokal gespeichert.

2. ERSTE SCHRITTE

Die GravityZone-Funktionen können über eine zentrale Verwaltungsplattform namens Control Center konfiguriert und verwaltet werden. Control Center hat eine Web-basierte Oberfläche, auf die Sie mit einem Benutzernamen und einem Passwort zugreifen können.

2.1. Verbinden mit dem Control Center

Der Zugriff auf die Control Center erfolgt über Benutzerkonten. Sie erhalten Ihre Anmeldeinformationen per E-Mail, sobald Ihr Konto angelegt wurde.

Vorbereitende Maßnahmen:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+
- Empfohlene Bildschirmauflösung: 1024x768 oder höher.

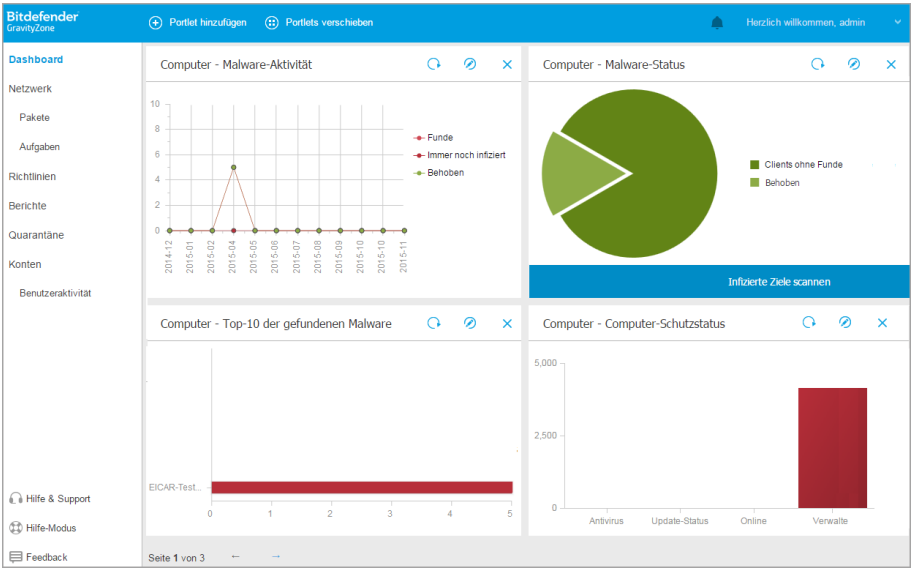
So stellen Sie eine Verbindung zum Control Center her:

1. Öffnen Sie Ihren Internet-Browser.
2. Rufen Sie die folgende Seite auf: https://gravityzone.bitdefender.com
3. Geben Sie die E-Mail-Adresse und das Passwort für Ihr Konto ein.
4. Klicken Sie auf **Anmelden**.

Beachten Sie
Sollten Sie Ihr Passwort vergessen haben, verwenden Sie den Link für die Passwortwiederherstellung, um ein neues Passwort anzufordern. Sie müssen die E-Mail-Adresse Ihres Kontos angeben.

2.2. Control Center auf einen Blick

Control Center ist so aufgebaut, dass Sie schnellen Zugriff auf alle Funktionen erhalten. Verwenden Sie die Menüleiste auf der rechten Seite, um durch die Konsole zu navigieren. Welche Funktionen zur Verfügung stehen, hängt davon ab, welcher Benutzertyp auf die Konsole zugreift.



Das Dashboard

2.2.1. Übersicht über die Control Center

Benutzer mit Unternehmensadministratorrolle haben Zugriff auf Netzwerksicherheitseinstellungen und auf die Unternehmensdetails (z. B. die Lizenz), während die Rechte von Administratorkonten sich hauptsächlich auf Netzwerksicherheitseinstellungen beziehen.

Je nach ihrer Rolle können GravityZone-Administratoren auf folgende Bereiche aus der Menüleiste zugreifen:

Dashboard

Übersichtliche Diagramme anzeigen, die wichtige Sicherheitsinformationen über Ihr Netzwerk enthalten.

Netzwerk
Schutz installieren, Richtlinien zur Verwaltung von Sicherheitseinstellungen anwenden, Aufgaben aus der Ferne ausführen und Schnellberichte erstellen.

Richtlinien
Sicherheitsrichtlinien erstellen und verwalten.

Berichte
Sicherheitsberichte über verwaltete Clients erhalten.

Quarantäne
Dateien in Quarantäne per Fernzugriff verwalten.

Konten
Zugriff zum Control Center anderer Mitarbeiter der Unternehmens verwalten.

> **Beachten Sie**
> Dieses Menü steht nur Benutzern zur Verfügung, die das Recht haben, Benutzer zu verwalten.

In diesem Menü finden Sie auch die Seite **Benutzeraktivität**, über die Sie auf das Aktivitätsprotokoll zugreifen können.

Außerdem erhalten Sie oben rechts in der Konsole über das Symbol **Benachrichtigungen** schnellen Zugriff auf die Seite **Benachrichtigungen**.

Wenn Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole klicken, erhalten Sie die folgenden Optionen:

- **Mein Konto**. Klicken Sie auf diese Option, um Ihre Benutzerkontoinformationen und -einstellungen zu bearbeiten.
- **Mein Unternehmen**. Klicken Sie auf diese Option, um Ihre Unternehmenskontoinformationen und -einstellungen zu verwalten.
- **Zugangsdaten-Manager**. Klicken Sie auf diese Option, um die für Ferninstallationsaufgaben nötigen Authentifizierungsdaten hinzuzufügen und zu verwalten.
- **Abmelden**. Klicken Sie auf diese Option, um sich bei Ihrem Konto abzumelden.

In der linken unteren Ecke der Konsole stehen die folgenden Links zur Verfügung:

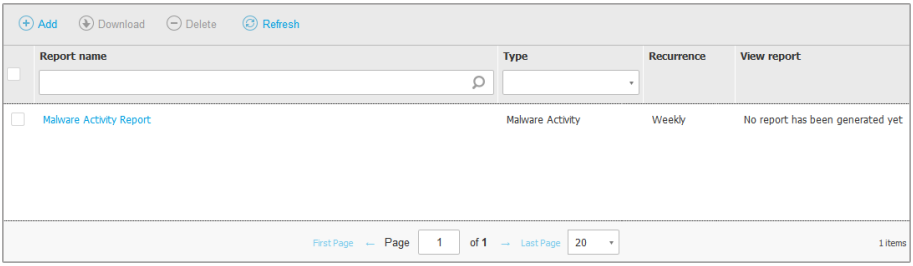
- **Hilfe und Support**. Klicken Sie auf diese Schaltfläche, um Hilfe- und Support-Informationen zu erhalten.
- **Hilfe-Modus**. Klicken Sie auf diese Schaltfläche, um die Hilfefunktion zu aktivieren, mit der vergrößerbare Tooltipps für Control Center-Objekte angezeigt

werden. Dadurch erhalten Sie nützliche Informationen zu den Funktionen des Control Center.

- **Feedback**. Klicken Sie auf diese Schaltfläche, um ein Formular anzuzeigen, in dem Sie uns Rückmeldung zu Ihren Erfahrungen mit GravityZone zusenden können.

2.2.2. Tabellendaten

Tabellen kommen in der Konsole häufig zum Einsatz, um die Daten in einem übersichtlichen Format zu organisieren.



Die Berichteseite - Berichtstabelle

Durch Tabellenseiten blättern

Tabellen mit mehr als 20 Einträgen haben mehr als eine Seite. Standardmäßig werden nur 20 Einträge pro Seite angezeigt. Verwenden Sie die Navigationsschaltflächen am unteren Rand der Tabelle, um zwischen den Seiten zu wechseln. Sie können die Anzahl der Einträge, die pro Seite angezeigt werden, ändern, indem Sie eine andere Option aus dem Menü neben den Navigationsschaltflächen wählen.

Nach bestimmten Einträgen suchen

Über die Suchfelder unter den Spaltenüberschriften können Sie leicht bestimmte Einträge finden.

Geben Sie den Suchbegriff in das entsprechende Feld ein. Passende Suchtreffer werden bereits während der Eingabe in der Tabelle angezeigt. Um den Inhalt der Tabelle wieder herzustellen, löschen Sie einfach die Suchfelder.

Daten sortieren

Sie können die Daten in der Tabelle nach dem Inhalt einer bestimmten Spalte sortieren, indem Sie auf die entsprechende Spaltenüberschrift klicken. Mit einem erneuten Klick auf die Spaltenüberschrift kehren Sie die Sortierreihenfolge um.

Tabellendaten neu laden

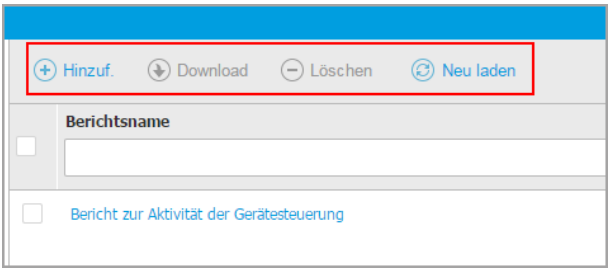
Um sicherzustellen, dass die aktuellsten Informationen angezeigt werden, klicken Sie am oberen Rand der Tabelle auf **Neu laden**.

Dies könnte notwendig werden, wenn Sie mehr Zeit auf der Seite verbringen.

2.2.3. Symbolleisten

Im Control Center können Sie über Symbolleisten bestimmte Operationen ausführen, die zu dem Bereich gehören, indem Sie sich gerade befinden. Jede Symbolleiste besteht aus mehreren Symbolen, die meistens am oberen Rand der Tabelle angezeigt werden. Über die Symbolleiste im Bereich **Berichte** können Sie zum Beispiel die folgenden Aktionen ausführen:

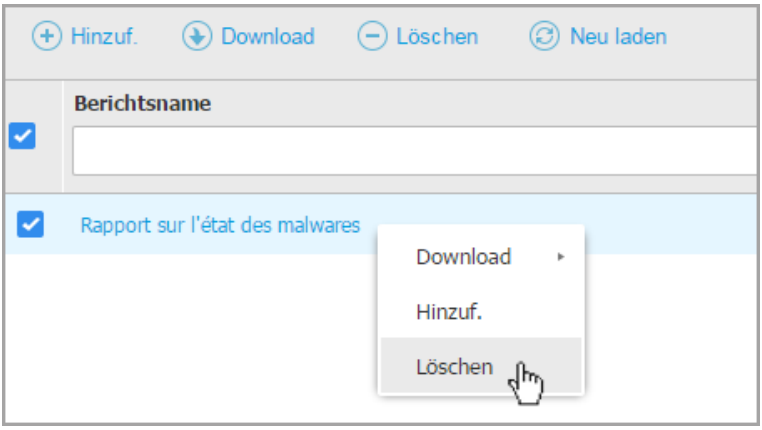
- Neuen Bericht erstellen.
- Einen geplanten Bericht herunterladen.
- Einen geplanten Bericht löschen.



Die Berichteseite - Symbolleiste

2.2.4. Kontextmenü

Die Symbolleistenbefehle stehen auch über das Kontextmenü zur Verfügung. Klicken Sie mit der rechten Maustaste auf den Bereich des Control Centers, den Sie gerade benutzen, und wählen Sie den gewünschten Befehl aus der Liste.

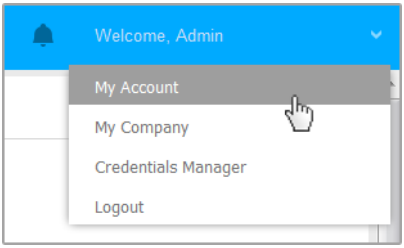


Die Berichteseite - Kontextmenü

2.3. Verwalten Ihres Kontos

So überprüfen oder ändern Sie Ihre Kontodetails und -Einstellungen:

1. Klicken Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole, und wählen Sie **Mein Konto**.



Das Benutzerkontomenü

2. Korrigieren oder aktualisieren Sie Ihre Kontoinformationen unter **Kontodetails**.
   - **Vollständiger Name.** Geben Sie Ihren vollen Namen ein.
   - **E-Mail.** Dies ist Ihre E-Mail-Adresse für die Anmeldung und den Kontakt. An diese Adresse werden Berichte und wichtige Sicherheitsbenachrichtigungen geschickt. Es werden automatisch E-Mail-Benachrichtigungen versandt, sobald wichtige Risikobedingungen im Netzwerk erkannt werden.

- Über den Link **Passwort ändern** können Sie Ihr Anmeldepasswort ändern.

3. Konfigurieren Sie die Kontoeinstellungen unter **Einstellungen** nach Ihren Wünschen.
   - **Zeitzone.** Wählen Sie im Menü die Zeitzone für Ihr Konto. Die Konsole zeigt die aktuelle Zeit entsprechend der ausgewählten Zeitzone.
   - **Sprache.**Wählen Sie im Menü die Anzeigesprache für die Konsole aus.
   - **Zeitüberschreitung der Sitzung.** Legen Sie den Inaktivitätszeitraum fest, nach dem Ihre Sitzung abläuft.
4. Klicken Sie **Speichern**, um die Änderungen zu speichern.

Beachten Sie
Sie können Ihr eigenes Konto nicht löschen.

2.4. Ändere Login Passwort

Nachdem Ihr Konto angelegt wurde, erhalten Sie eine E-Mail mit den Anmeldedaten.

Es empfiehlt sich, wie folgt vorzugehen:

- Ändern Sie das Standardpasswort nach dem ersten Aufrufen von Control Center.
- Ändern Sie Ihr Kennwort regelmäßig.

Um das Anmeldepasswort zu ändern:

1. Klicken Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole, und wählen Sie **Mein Konto**.
2. Klicken Sie unter **Kontodetails** auf **Passwort ändern**.
3. Geben Sie Ihr aktuelles Passwort und das neue Passwort in die entsprechenden Felder ein.
4. Klicken Sie **Speichern**, um die Änderungen zu speichern.

2.5. Ihr Unternehmen verwalten

Als Nutzer mit der Rolle Unternehmens-Administrator können Sie die Details Ihres Unternehmens und Ihre Lizenz-Einstellungen einsehen oder ändern:

1. Klicken Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole, und wählen Sie **Mein Unternehmen**.
2. Geben Sie im Bereich **Unternehmensdetails** Informationen wie den Namen, die Adresse und die Telefonnummer Ihres Unternehmens ein.

So können Sie das Logo, das im Control Center und in den Berichten und E-Mails Ihres Unternehmens angezeigt wird, ändern:

- Klicken Sie auf **Ändern**, um das Logobild auf Ihrem Computer zu suchen. Das Dateiformat muss entweder PNG oder JPG sein, und das Bild muss genau 200×30 Pixel groß sein.
- Klicken Sie auf **Standard**, um das Bild zu löschen und wieder das von Bitdefender bereitgestellte Bild zu verwenden.

3. Ihr Unternehmen kann standardmäßig über die Partnerkonten anderer Unternehmen verwaltet werden, die Ihr Unternehmen vielleicht in ihrer Bitdefender Control Center gelistet haben Sie können den Zugriff dieser Unternehmen auf Ihr Netzwerk blockieren, indem Sie die Option **Partnern erlauben, bei der Verwaltung der Sicherheit dieses Unternehmens zu helfen** deaktivieren. Danach wird Ihr Netzwerk nicht mehr in der Control Center anderer Unternehmen angezeigt und diese können Ihr Abonnement nicht mehr verwalten.
4. Im Bereich **Lizenz** können Sie Ihre Lizenzinformationen einsehen und verändern.
   - So fügen Sie einen neuen Lizenzschlüssel hinzu:
     a. Wählen Sie im Menü **Typ** den Abonnementtyp **Lizenz** aus.
     b. Geben Sie im Feld **Lizenzschlüssel** den Lizenzschlüssel ein.
     c. Klicken Sie auf die **Überprüfen**-Schaltfläche und warten Sie, bis die Control Center die Informationen über den eingegebenen Lizenzschlüssel abgerufen hat.
   - Unter dem Lizenzschlüssel werden Informationen zu diesem Lizenzschlüssel angezeigt:
     – **Ablaufdatum**: das Datum, bis zu dem der Lizenzschlüssel verwendet werden kann.
     – **Benutzt**: die Anzahl der benutzten Arbeitsplätze im Verhältnis zur Anzahl der im Lizenzschlüssel vorgesehenen Arbeitsplätze. Ein Arbeitsplatz gilt als benutzt, wenn der Bitdefender-Client auf einem Endpunkt in dem von Ihnen verwalteten Netzwerk installiert wurde.
     – **Kann installiert werden**: die Anzahl der verfügbaren Arbeitsplätze im Verhältnis zu den Arbeitsplätzen einer monatlichen Lizenz (benutzte Arbeitsplätze nicht mitgezählt).
     – **Gesamt**: die Gesamtzahl an Arbeitsplätzen, die Ihre Lizenz beinhaltet.

5. Unter **Bitdefender Partner** finden Sie Informationen zu Ihrem Dienstleister.

   So wechseln Sie Ihren Managed-Service-Anbieter:

   a. Klicken Sie auf die Schaltfläche **Ändern**.

   b. Geben Sie die Kennung des Partnerunternehmens im Feld **Partnerkennung** ein.

      Beachten Sie
      Unternehmen können ihre Kennung auf der Seite **Mein Unternehmen** einsehen. Wenn Sie eine Vereinbarung mit einem Partnerunternehmen getroffen haben, muss ein Unternehmensvertreter Ihnen die Control-Center-Kennung des Unternehmens mitteilen.

   c. Klicken Sie auf **Speichern**.

   Ihr Unternehmen wird so automatisch aus der Control Center des alten Partners in die des neuen Partners verschoben.

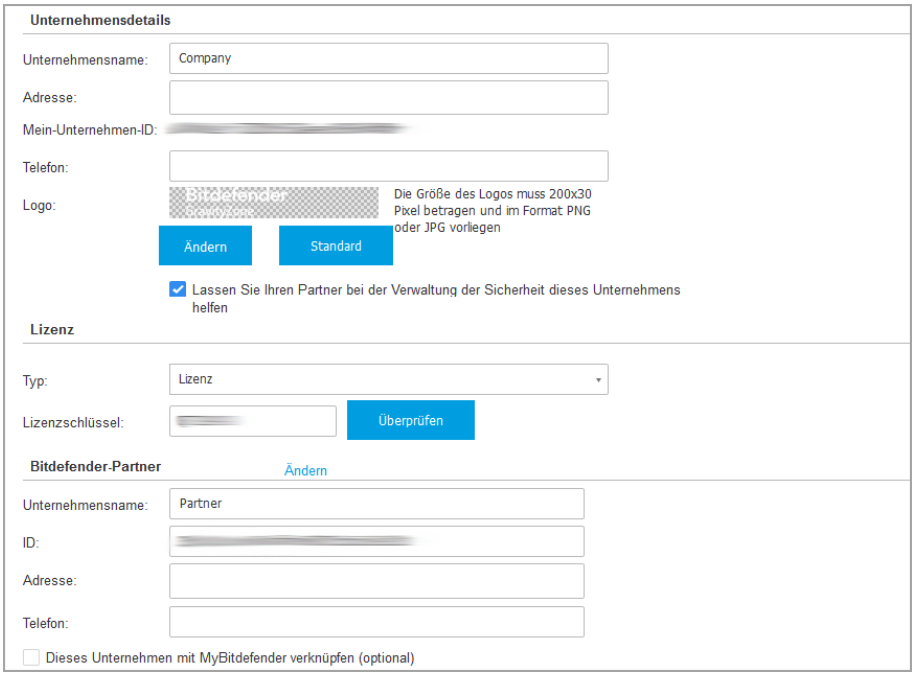
6. Wenn Sie möchten, können Sie über die entsprechenden Felder Ihr Unternehmen mit Ihrem MyBitdefender-Konto verknüpfen.
7. Klicken Sie **Speichern**, um die Änderungen zu speichern.

3. BENUTZERKONTEN VERWALTEN

Der Security for Endpoints-Dienst kann über die Control Center mit dem Konto eingerichtet und verwaltet werden, das Ihnen nach der Anmeldung für den Dienst zugewiesen wurde.

Mit den folgenden Punkten zu den GravityZone-Benutzerkonten sollten Sie vertraut sein:

- Sie können interne Benutzerkonten anlegen, um anderen Mitarbeitern im Unternehmen Zugriff auf die Control Center zu ermöglichen. Sie können Benutzerkonten verschiedene Rollen mit unterschiedlichen Zugriffsrechten zuweisen.
- Für jedes Benutzerkonto können Sie den Zugriff auf GravityZone-Funktionen oder bestimmte Teile des Netzwerks, zu dem es gehört, festlegen.
- Alle Konten mit der Berechtigung **Benutzer verwalten** können andere Konten erstellen, bearbeiten und löschen.
- Sie können ausschließlich Konten verwalten, die die gleichen oder weniger Rechte wie Ihr eigenes Konto haben.
- Auf der Seite **Konten** können Sie Benutzerkonten erstellen und verwalten.



Die Kontenübersicht

Bestehende Konten werden in der Tabelle angezeigt. Sie können das Folgende für jedes Benutzerkonto einsehen:

- Benutzername des Kontos.
- E-Mail-Adresse des Kontos (die zur Anmeldung am Control Center verwendet wird). An diese Adresse werden Berichte und wichtige Sicherheitsbenachrichtigungen geschickt. Es werden automatisch E-Mail-Benachrichtigungen versandt, sobald wichtige Risikobedingungen im Netzwerk erkannt werden.
- Benutzerrolle (Unternehmensadministrator / Netzwerkadministrator / Berichterstatter / benutzerdefiniert)

3.1. Benutzerrollen

Eine Benutzerrolle umfasst eine bestimmte Kombination aus Benutzerrechten. Wenn Sie ein Benutzerkonto anlegen, können Sie eine der vordefinierten Rollen wählen oder eine benutzerdefinierte Rolle erstellen, indem Sie nur die gewünschten Benutzerrechte auswählen.

Beachten Sie
Sie können anderen Benutzerkonten nur die Rechte zuweisen, über die Sie selbst verfügen.

Die folgenden Benutzerrollen sind verfügbar:

1. **Unternehmensadministrator** - Geeignet für Manager von Kundenunternehmen, die eine GravityZone-Lizenz von einem Partner erworben haben. Ein Unternehmensadministrator verwaltet die Lizenz, das Unternehmensprofil und die gesamte GravityZone-Installation. Er erhält somit umfassende Kontrolle über alle Sicherheitseinstellungen (es sei denn, dies wurde im Rahmen eines Dienstleisterszenarios von dem übergeordneten Partnerkonto außer Kraft gesetzt). Unternehmensadministratoren können ihre Aufgaben mit untergeordneten Administrator- und Berichterstatterkonten teilen oder diese an sie delegieren.
2. **Netzwerkadministrator** - Für ein Unternehmen können mehrere Benutzerkonten mit der Netzwerkadministrator-Rolle angelegt werden. Diese verfügen über Administratorrechte für alle Sicherheitsagenten im Unternehmen bzw. für eine festgelegte Gruppe von Endpunkten; das schließt die Benutzerverwaltung ein. Netzwerkadministratoren sind zuständig für die aktive Verwaltung der Sicherheitseinstellungen im Netzwerk.
3. **Berichterstatter** - Berichterstatterkonten sind interne Konten, die ausschließlich über Lesezugriff verfügen. Über sie erhält man nur Zugriff auf Berichte und Protokolle. Diese Benutzerkonten können Mitarbeitern bereitgestellt werden, die Überwachungsaufgaben wahrnehmen oder über die Sicherheitslage auf dem Laufenden gehalten werden müssen.
4. **Benutzerdefiniert** - Vordefinierte Benutzerrollen beinhalten eine bestimmte Kombination aus Berechtigungen. Sollte eine vordefinierte Benutzerrolle Ihren Anforderungen nicht entsprechen, können Sie ein benutzerdefiniertes Konto mit genau den Rechten anlegen, die Sie benötigen.

Die nachfolgende Tabelle gibt einen Überblick über die Zusammenhänge zwischen den verschiedenen Rollen und ihren Berechtigungen. Detaillierte Informationen finden Sie unter „Benutzerrechte“ (S. 20).

Rolle des Kontos	Zugelassene untergeordnete Konten	Benutzerrechte
Unternehmensadministrator	Unternehmensadministratoren, Netzwerkadministratoren, Berichterstatter	Eigenes Unternehmen verwalten Benutzer verwalten Netzwerke verwalten Berichte verwalten
Netzwerkadministrator	Netzwerkadministratoren, Berichterstatter	Benutzer verwalten Netzwerke verwalten Berichte verwalten
Berichterstatter	-	Berichte verwalten

3.2. Benutzerrechte

Sie können den GravityZone-Benutzerkonten die folgenden Benutzerrechte zuweisen:

- **Benutzer verwalten**. Benutzerkonten erstellen, bearbeiten oder löschen.
- **Eigenes Unternehmen verwalten**. Benutzer können ihren eigenen GravityZone-Lizenzschlüssel verwalten und die Einstellungen für ihr Unternehmensprofil bearbeiten. Dieses Recht haben nur Unternehmensadministratoren.
- **Netzwerke verwalten**. Gewährt Administrationsrechte über die Netzwerksicherheitseinstellungen (Netzwerkinventar, Richtlinien, Aufgaben, Installationspakete, Quarantäne). Dieses Recht haben nur Netzwerkadministratoren.
- **Berichte verwalten**. Berichte anlegen, bearbeiten, löschen und das Dashboard verwalten.

3.3. Benutzerkonten erstellen

Bevor Sie ein Benutzerkonto anlegen, sollten Sie sicherstellen, dass Sie die benötigte E-Mail-Adresse zur Hand haben. Diese Adresse wird zwingend für das Anlegen des GravityZone-Benutzerkontos benötigt. Den Benutzern werden ihre GravityZone-Zugangsdaten an die angegebene E-Mail-Adresse gesendet. Benutzer werden die E-Mail-Adresse auch für die GravityZone-Anmeldung verwenden.

Um ein Benutzerkonto anzulegen:

1. Rufen Sie die Seite **Konten** auf.
2. Klicken Sie auf die Schaltfläche ⊕**Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird geöffnet.
3. Geben Sie im Bereich **Details** die Benutzerkontoinformationen ein.
   - **E-Mail**. Geben Sie die E-Mail-Adresse des Benutzers ein. Die Anmeldeinformationen werden an diese E-Mail-Adresse versandt, sobald das Konto angelegt wurde.

     Beachten Sie
     Die E-Mail-Adresse darf nur einmal vergeben werden. Sie können keine weiteren Benutzerkonten mit der gleichen E-Mail-Adresse anlegen.

   - **Vollständiger Name**. Geben Sie den vollständigen Namen des Kontoinhabers ein.
4. Konfigurieren Sie im Bereich **Einstellungen und Rechte** die folgenden Einstellungen:
   - **Zeitzone**. Wählen Sie im Menü die Zeitzone für das Konto. Die Konsole zeigt die aktuelle Zeit entsprechend der ausgewählten Zeitzone.
   - **Sprache**. Wählen Sie im Menü die Anzeigesprache für die Konsole aus.
   - **Rolle**. Wählen Sie die Rolle des Benutzers aus. Weitere Details zu Benutzerrollen finden Sie unter „Benutzerrollen“ (S. 19).
   - **Rechte**. Jede vordefinierte Benutzerrolle verfügt über einen bestimmten Satz von Rechten. Sie können dabei aber genau die Rechte auswählen, die Sie benötigen. Die Benutzerrolle wechselt dann zu **Benutzerdefiniert**. Weitere Informationen zu den Benutzerrechten finden Sie unter „Benutzerrechte“ (S. 20).

- **Ziele wählen**. Wählen Sie die Netzwerkgruppen aus, auf die der Benutzer Zugriff haben wird.

  Sie können den Benutzerzugriff auf bestimmte Netzwerkbereiche beschränken.

5. Klicken Sie auf **Speichern**, um den Benutzer hinzuzufügen. Das neue Konto erscheint in der Liste der Benutzerkonten.

> **Beachten Sie**
> Das Passwort für jedes Benutzerkonto wird automatisch nach Anlegen des Kontos vergeben und gemeinsam mit den anderen Kontodaten an die E-Mail-Adresse des Benutzers gesendet.
> Sie können das Passwort nach Anlegen des Kontos ändern. Klicken Sie in der **Konten**-Übersicht auf den Kontonamen, um das Passwort zu bearbeiten. Benutzer werden per E-Mail umgehend über die Änderung des Passworts informiert.
> Benutzer können ihr Anmeldepasswort über die Control Center ändern, indem Sie die Seite **Mein Konto** aufrufen.

3.4. Konten bearbeiten

Bearbeiten Sie Konten, um die Kontoinformationen auf dem neuesten Stand zu halten oder die Kontoeinstellungen anzupassen.

Um ein Benutzerkonto zu bearbeiten:

1. Melden Sie sich an der Control Center an.
2. Rufen Sie die Seite **Konten** auf.
3. Klicken Sie auf den Benutzernamen.
4. Ändern Sie die Kontoinformationen und -einstellungen nach Bedarf.
5. Klicken Sie **Speichern**, um die Änderungen zu speichern.

> **Beachten Sie**
> Alle Konten mit der Berechtigung **Benutzer verwalten** können andere Konten erstellen, bearbeiten und löschen. Sie können ausschließlich Konten verwalten, die die gleichen oder weniger Rechte wie Ihr eigenes Konto haben.

3.5. Benutzerkonten löschen

Löschen Sie Konten, wenn diese nicht mehr benötigt werden. So zum Beispiel wenn ein Kontoinhaber das Unternehmen verlassen hat.

Um ein Konto zu löschen:

1. Melden Sie sich an der Control Center an.
2. Rufen Sie die Seite **Konten** auf.
3. Wählen Sie das Konto aus der Liste aus.
4. Klicken Sie auf die Schaltfläche ⊖ **Löschen** am oberen Rand der Tabelle.

   Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

3.6. Anmeldepasswörter zurücksetzen

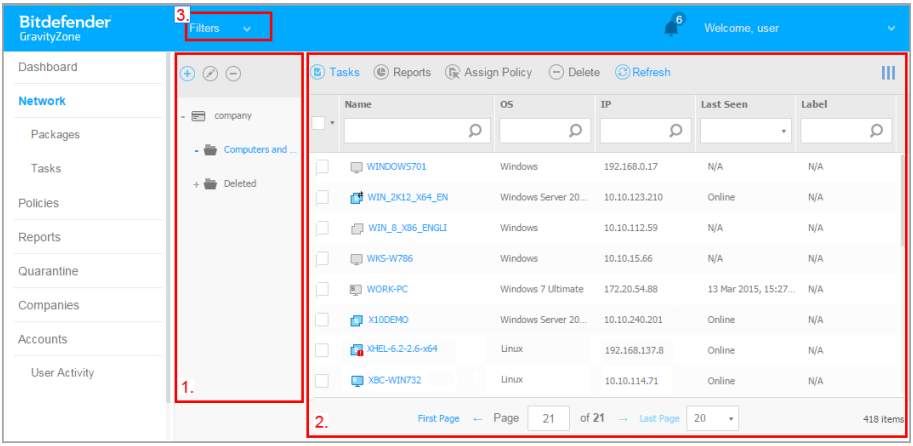
Kontoinhaber, die ihr Passwort vergessen haben, können es über den Link für die Passwortwiederherstellung auf der Anmeldeseite zurücksetzen. Sie können ein vergessenes Anmeldepasswort auch zurücksetzen, indem Sie das entsprechende Konto über die Konsole bearbeiten.

Um das Anmeldepasswort für einen Benutzer zurückzusetzen:

1. Melden Sie sich an der Control Center an.
2. Rufen Sie die Seite **Konten** auf.
3. Klicken Sie auf den Benutzernamen.
4. Geben Sie in die entsprechenden Felder ein neues Passwort ein (unter **Details**).
5. Klicken Sie **Speichern**, um die Änderungen zu speichern. Der Kontoeigentümer erhält dann eine E-Mail mit dem neuen Passwort.

4. ENDPUNKTE VERWALTEN

Auf der Seite **Netzwerk** finden sich viele Funktionen zum Durchsuchen und Verwalten der verfügbaren Endpunkte. Der Bereich **Netzwerk** besteht aus zwei Fenstern, in denen der Status aller Netzwerkobjekte in Echtzeit angezeigt wird.



Die Netzwerk-Übersicht

1. Im linken Fenster werden die verfügbaren Netzwerke in Baumansicht angezeigt.

   Alle gelöschten Endpunkte sind im Ordner **Gelöscht** gespeichert. Weitere Informationen finden Sie unter „Endpunkte aus dem Netzwerkinventar löschen“ (S. 58).

   Beachten Sie
   Sie können nur diejenigen Gruppen verwalten, für die Sie Administratorrechte haben.

2. Im rechten Fenster wird der Inhalt der Gruppe, die Sie im Netzwerkbaum ausgewählt haben, angezeigt. Dieses Fenster besteht aus einem Raster, in dem in jeder Zeile ein Netzwerkobjekt steht und in jeder Spalte bestimmte Informationen zu diesen Objekten.

   In diesem Fenster können Sie Folgendes tun:

- Detaillierte Informationen zu jedem Netzwerkobjekt in Ihrem Konto einsehen. Der Status jedes Objekts wird durch das Symbol neben seinem Namen angezeigt. Klicken Sie auf den Namen des Objekts, um ein Fenster mit weiteren Informationen anzuzeigen.

  Jede Art von Objekt, z. B. Computer, virtuelle Maschine oder Ordner, wird durch ein bestimmtes Symbol dargestellt. Jedes Netzwerkobjekt hat außerdem einen bestimmten Status in Bezug auf Verwaltungszustand, Sicherheitsprobleme, Netzwerkverbindung usw. Nähere Details zur Beschreibung jedes Netzwerkobjektsymbols und der jeweiligen Zustände finden Sie unter „Netzwerkobjekttypen und -status“ (S. 175).

- Über die Symbolleiste am oberen Rand der Tabelle können Sie bestimmte Operationen für jedes Netzwerkobjekt ausführen (z. B. Aufgaben ausführen, Berichte erstellen Richtlinien zuweisen und löschen) und die Tabellendaten neu laden.

3. The **Filter**

Im Bereich **Netzwerk** können Sie auch die Installationspakete sowie die Aufgaben für jeden Netzwerkobjekttyp verwalten.

Beachten Sie
Weitere Informationen zu Installationspaketen finden Sie in der GravityZone-Installationsanleitung.

Um die Endpunkte anzuzeigen, die zu Ihrem Konto gehören, öffnen Sie die Seite **Netzwerk** und wählen Sie die gewünschte Netzwerkgruppe im linken Fenster aus.

Im linken Fenster sehen Sie die verfügbare Netzwerkstruktur und im rechten Fenster Details zu jedem Endpunkt.

Zunächst werden alle in Ihrem Netzwerk gefundenen Computer und virtuellen Maschinen als nicht verwaltet angezeigt, damit Sie per Fernzugriff die Sicherheitssoftware auf ihnen installieren können.

So passen Sie die Endpunktdetails an, die in der Tabelle angezeigt werden:

1. Klicken Sie auf die Schaltfläche **Spalten** rechts oben im rechten Fenster.
2. Wählen Sie die Spalten, die Sie anzeigen möchten.
3. Klicken Sie auf die Schaltfläche **Zurücksetzen**, um zur Standardansicht zurückzukehren.

Auf der Seite **Netzwerk** stehen Ihnen folgende Verwaltungsoptionen für Endpunkte zur Verfügung:

- Den Status des Endpunkts überprüfen
- Endpunktdetails anzeigen
- Endpunkte in Gruppen organisieren.
- Sortieren, filtern und suchen
- Aufgaben ausführen
- Schnellberichte erstellen
- Regeln zuweisen
- Endpunkte aus dem Netzwerkinventar löschen

Um die neuesten Informationen in der Tabelle anzuzeigen, klicken Sie im unteren linken Bereich der Tabelle auf **Neu laden**. Dies könnte notwendig werden, wenn Sie mehr Zeit auf der Seite verbringen.

4.1. Status der Endpunkts überprüfen

Jeder Endpunkt wird auf der Netzwerkseite seinem Typ und Status entsprechend durch ein Symbol dargestellt.

Unter „Netzwerkobjekttypen und -status“ (S. 175) finden Sie eine Liste aller Symbole und Status.

Detaillierte Statusinformationen finden Sie unter:

- Endpunktverwaltungsstatus
- Endpunktverbindungsstatus
- Endpunktsicherheitsstatus

4.1.1. Endpunktverwaltungsstatus

Endpunkte haben immer einen der folgenden Verwaltungsstatus:

- **Verwaltet** - Endpunkte, auf denen der Sicherheitsagent installiert ist.
- **Nicht verwaltet** - gefundene Endpunkte, auf denen der Sicherheitsagent noch nicht installiert wurde.
- **Gelöscht** - Endpunkte, die Sie aus dem Control Center gelöscht haben. Weitere Informationen finden Sie unter „Endpunkte aus dem Netzwerkinventar löschen“ (S. 58).

4.1.2. Endpunktverbindungsstatus

Der Verbindungsstatus betrifft alle virtuellen Maschinen und nur die verwalteten Computer. Verwaltete Endpunkte können einen der folgenden Status haben:

- **Online**. Ein blaues Symbol zeigt an, dass der Endpunkt online ist.
- **Offline**. Ein graues Symbol zeigt an, dass der Endpunkt offline ist.

Ein Endpunkt gilt als offline, wenn der Sicherheitsagent länger als 5 Minuten inaktiv ist. Mögliche Gründe, weshalb Endpunkte als offline angezeigt werden:

- Der Endpunkt ist ausgeschaltet, im Ruhezustand oder im Energiesparmodus.

  Beachten Sie
  Endpunkte werden auch dann als online angezeigt, wenn sie gesperrt sind oder der Benutzer sich abgemeldet hat.

- Der Sicherheitsagent hat keine Verbindung zum Bitdefender Control Center oder zum zugewiesenen Endpoint Security Relay:
  - Die Verbindung des Endpunkts zum Netzwerk könnte unterbrochen worden sein.
  - Eine Netzwerk-Firewall oder ein Router könnte die Kommunikation zwischen dem Sicherheitsagenten und dem Bitdefender Control Center oder dem zugewiesenen Endpoint Security Relay blockieren.
  - Der Endpunkt befindet sich hinter einem Proxy-Server, und in der zugewiesenen Richtlinie wurden die Proxy-Einstellungen nicht korrekt konfiguriert.

    Warnung
    Bei Endpunkten hinter einem Proxy-Server müssen die Proxy-Einstellungen im Installationspaket des Sicherheitsagenten korrekt konfiguriert sein, da der Endpunkt sonst nicht mit der GravityZone kommunizieren kann und immer als offline angezeigt wird, selbst wenn nach der Installation eine Richtlinie mit den korrekten Proxy-Einstellungen angewendet wird.

- Der Sicherheitsagent wurde manuell deinstalliert, während der Computer nicht mit dem GravityZone Control Center verbunden war. Normalerweise wird das Control Center über die manuelle Deinstallation des Sicherheitsagenten von einem Computer benachrichtigt und der Computer wird als nicht verwaltet gekennzeichnet.
- Der Sicherheitsagent funktioniert unter Umständen nicht richtig.

So finden Sie heraus, wie lange Endpunkte inaktiv waren:

1. Zeigen Sie nur die verwalteten Endpunkte an. Klicken Sie am oberen Rand der Tabelle auf das Menü **Filter**, wählen Sie im Reiter **Sicherheit** alle gewünschten "Verwaltet"-Optionen, markieren Sie dann im Reiter **Tiefe** die Option **Alle Objekte rekursiv** und klicken Sie anschließend auf **Speichern**.
2. Klicken Sie auf die Spaltenüberschrift **Zuletzt gesehen**, um die Endpunkte nach dem Zeitraum ihrer Inaktivität zu sortieren.

Sie können kürzere Inaktivitätszeiträume (Minuten, Stunden) ignorieren, da diese vermutlich auf ein temporäres Problem zurückzuführen sind. Der Endpunkt ist zum Beispiel gerade ausgeschaltet.

Längere Inaktivitätszeiträume (Tage, Wochen) deuten in der Regel auf ein Problem mit dem Endpunkt hin.

Beachten Sie
Wir empfehlen, die Netzwerktabelle immer mal wieder neu zu laden, damit die jeweils aktuellen Daten angezeigt werden.

4.1.3. Endpunktsicherheitsstatus

Der Sicherheitsstatus betrifft nur verwaltete Endpunkte. Endpunkte mit Sicherheitsproblemen erkennen Sie daran, dass ein Warnsymbol am Statussymbol angezeigt wird:

- Computer verwaltet, mit Problemen, online.
- Computer verwaltet, mit Problemen, offline.

Ein Endpunkt hat dann Sicherheitsprobleme, wenn mindestens einer der folgenden Punkte zutrifft:

- Malware-Schutz ist deaktiviert.
- Der Lizenzzeitraum ist abgelaufen.
- Der Sicherheitsagent ist veraltet.
- Die Malware-Signaturen sind veraltet.
- Malware wurde gefunden.
- Die Verbindung mit Bitdefender Cloud Services konnte nicht hergestellt werden. Mögliche Gründe hierfür sind:
  - Eine Netzwerk-Firewall blockiert die Verbindung mit Bitdefender Cloud Services.
  - Port 80, der für die Kommunikation mit Bitdefender Cloud Services verwendet wird, ist geschlossen.

In diesem Fall läuft der Malware-Schutz allein auf Grundlage der lokalen Engines. Cloud-Scans sind ausgeschaltet. Das heißt, dass der Sicherheitsagent keinen umfassenden Echtzeitschutz gewährleisten kann.

Wenn Ihnen ein Endpunkt mit Sicherheitsproblemen auffällt, klicken Sie auf seinen Namen, um das Fenster **Informationen** anzuzeigen. Sicherheitsprobleme erkennen Sie an diesem ! Symbol. Vergessen Sie dabei nicht, in jedem einzelnen Reiter der Seite nach Sicherheitsinformationen zu suchen. Weitere Details erfahren Sie, wenn Sie den Mauszeiger über das Symbol bewegen. Eventuell muss dem Problem auf lokaler Ebene weiter nachgegangen werden.

Beachten Sie
Wir empfehlen, die Netzwerktabelle immer mal wieder neu zu laden, damit die jeweils aktuellen Daten angezeigt werden.

4.2. Endpunktdetails anzeigen

Auf der Seite **Netzwerk** finden Sie detaillierte Informationen zu jedem Endpunkt, z. B. Betriebssystem, IP-Adresse und das Datum, an dem der Computer zuletzt gesehen wurde.

So erhalten Sie weitere Details zu einem Endpunkt:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster.

   Alle Endpunkte der gewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
3. Der Status eines Endpunktes ist durch ein Symbol klar gekennzeichnet. Detaillierte Informationen finden Sie unter „Status der Endpunkts überprüfen“ (S. 26).
4. Die einzelnen Spalten enthalten verschiedene Informationen zu jedem Endpunkt:
   - **Name**: Name des Endpunkts.
   - **FQDN**: der sog. Fully Quqlified Domain Name, der den Host-Namen und den Domain-Namen beinhaltet
   - **Betriebssystem**: auf dem Endpunkt installiertes Betriebssystem.
   - **IP**: IP-Adresse des Endpunktes.
   - **Zuletzt gesehen**: Details über den Verbindungsstatus des Endpunktes.

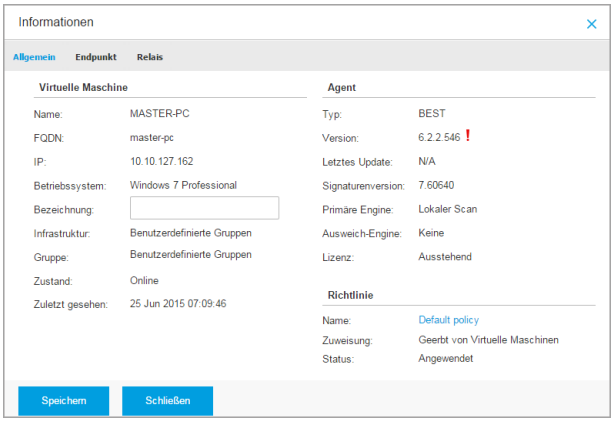
Beachten Sie
Sie sollten regelmäßig das Feld **Zuletzt gesehen** überprüfen, da lange Zeiträume der Inaktivität bedeuten können, dass Kommunikationsprobleme vorliegen oder der Computer vom Netzwerk getrennt wurde.

- **Bezeichnung**: die Bezeichnung, die dieser Endpunkt im Fenster **Information** trägt.

Beachten Sie
Sie können anpassen, welche Informationen in der Tabelle des rechten Fensters angezeigt werden, indem Sie rechts oben im rechten Fenster auf die Schaltfläche **Spalten** klicken. Sie können Spalten nach Bedarf hinzufügen und entfernen.

5. Klicken Sie auf den Namen des Endpunktes, der Sie interessiert. Das Fenster **Information** wird angezeigt.
   - Im Reiter **Allgemein** finden Sie die folgenden Details:
     - Allgemeine Informationen zum Endpunkt wie Name, FQDN-Informationen, IP-Adresse, Betriebssystem, Infrastruktur, übergeordnete Gruppe und aktueller Status. Sie können dem Endpunkt auch eine Bezeichnung zuweisen. So können Sie Endpunkte nach ihrer Bezeichnung suchen und filtern, indem Sie das Suchfeld der Spalte **Bezeichnung** in der Tabelle rechts auf der Seite **Netzwerk** verwenden.
     - Sicherheitsinformationen zum installierten Agenten, z. B. Agenttyp, Version, letztes Update, Produkt- und Signaturversionen, verwendete Malware-Schutz-Engines und Lizenzstatus.
     - Informationen zu einem mit Computern verbundenen Relais-Endpunkt (z. B. Name, IP-Adresse und Bezeichnung) finden Sie im Bereich **Mit dem Relais verbunden** .
     - Informationen zur zugewiesenen Richtlinie (Name, Zuweisungsmodus und Status). Klicken Sie auf den Namen der Richtlinie, um die Richtlinienvorlage und ihre Einstellungen anzuzeigen.

Beachten Sie
Jede Eigenschaft, die Sicherheitsprobleme bringt, ist mit dem Symbol ! markiert. Weitere Details erfahren Sie, wenn Sie den Mauszeiger über das Symbol bewegen. Eventuell muss dem Problem auf lokaler Ebene weiter nachgegangen werden.



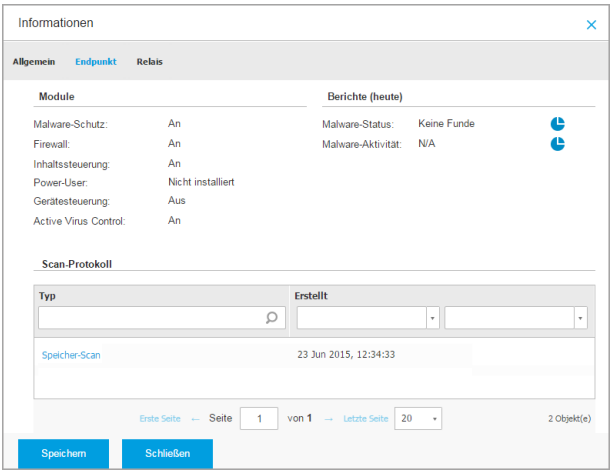
Information-Fenster - Allgemein

– Im Reiter **Endpunkt** finden Sie die folgenden Details:
  - Status der Sicherheitsmodule. Hier sehen Sie, welche Sicherheitsmodule auf dem Endpunkt installiert wurden, und welchen Status die verfügbaren Module (Ein/Aus) gemäß der angewendeten Richtlinie haben.
  - Ein kurzer Überblick über Malware-Berichte des heutigen Tages.

    Klicken Sie auf das Berichtsymbol, um die Malware-Bericht-Optionen für den ausgewählten Endpunkt aufzurufen.

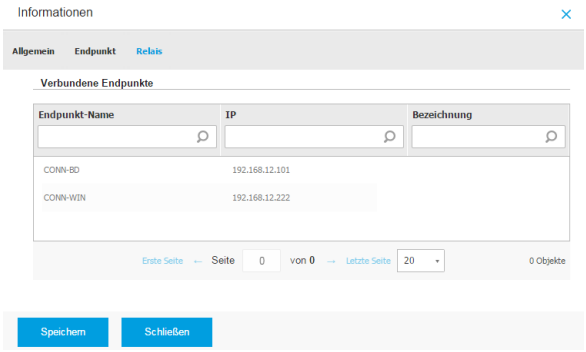
    Weitere Informationen finden Sie unter „Berichte erstellen“ (S. 144)
  - Im Bereich **Scan-Protokoll** werden detaillierte Informationen zu allen Scan-Aufgaben angezeigt, die auf dem Endpunkt ausgeführt wurden. Klicken Sie auf den gewünschten Scan, um das Scan-Protokoll in einer neuen Seite im Browser zu öffnen.

    Wenn mehrere Scan-Protokolle zur Verfügung stehen, können Sie sich über mehrere Seiten erstrecken. Über die Navigation am unteren Rand der Tabelle können Sie zwischen den Seiten wechseln. Wenn Sie sehr viele Einträge haben, können Sie die Filteroptionen über der Tabelle nutzen.



Information-Fenster - Endpunkt

– Der Reiter **Relais** steht nur für Endpunkte mit Relais-Rolle zur Verfügung. In diesem Reiter werden Informationen über Endpunkte angezeigt, die mit dem Relais verbunden sind, z. B. Name, IP-Adresse und Bezeichnung.



Information-Fenster - Relais

4.3. Endpunkte in Gruppen organisieren

Ein großer Vorteil dieser Funktion ist, dass Sie Gruppenrichtlinien verwenden können, um verschiedene Sicherheitsanforderungen zu erfüllen.

Sie können Endpunktgruppen im linken Fenster der Seite **Netzwerk** im Ordner **Computer und Gruppen** verwalten.

Unter der **Netzwerk**gruppe, die zu Ihrem Unternehmen gehört, können Sie Computer-Gruppen innerhalb einer benutzerdefinierten Baumstruktur erstellen, löschen, umbenennen und verschieben.

Beachten Sie

- Eine Gruppe kann sowohl Endpunkte als auch andere Gruppen enthalten.
- Wenn Sie im linken Fenster eine Gruppe auswählen, können Sie alle enthaltenen Endpunkt einsehen - außer denen, die in die jeweiligen Untergruppen eingeordnet wurden. Wenn Sie alle Endpunkte der Gruppe und ihrer Untergruppen anzeigen möchten, klicken Sie auf das Menü **Filter** am oberen Rand der Tabelle und wählen Sie **Alle Objekte rekursiv** im Bereich **Tiefe**.

Gruppen erstellen

Bevor Sie Gruppen erstellen, sollten Sie sich überlegen, warum Sie diese Gruppen brauchen und sie dann nach einem bestimmten System erstellen. Sie können Endpunkte zum Beispiel anhand von einem oder einer Kombination der folgenden Kriterien in Gruppen einteilen:

- Organisationsstruktur (Vertrieb, Marketing, Qualitätssicherung, Software-Entwicklung, Unternehmensführung usw.).
- Sicherheitsanforderungen (Desktop-Rechner, Laptops, Server usw.).
- Standort (Hauptsitz, Niederlassungen, mobile Angestellte, Heimarbeitsplätze usw.).

Um Ihr Netzwerk in Gruppen aufzuteilen:

1. Wählen Sie im rechten Fenster den Ordner **Computer und Gruppen**.
2. Klicken Sie auf die Schaltfläche ⊕ **Gruppe hinzufügen** im oberen Bereich des linken Fensters.
3. Geben Sie einen aussagekräftigen Namen für die Gruppe ein, und klicken Sie auf **OK**

Gruppen umbenennen

So benennen Sie eine Gruppe um:

1. Wählen Sie im linken Fenster die Gruppe aus.
2. Klicken Sie auf die Schaltfläche **Gruppe bearbeiten** im oberen Bereich des linken Fensters.
3. Geben Sie den neuen Namen in das entsprechende Feld ein.
4. Klicken Sie zur Bestätigung auf **OK**.

Gruppen und Endpunkte verschieben

Sie können Entitäten irgendwo innerhalb der Gruppenhierarchie nach **Computer und Gruppen** verschieben. Ziehen Sie die gewünschte Entität einfach mit der Maus aus dem rechten Fenster in die gewünschten Gruppe im linken Fenster.

Beachten Sie

Die Entität, die verschoben wird, erbt die Richtlinieneinstellungen der neuen übergeordneten Gruppe, sofern ihr keine abweichende Richtlinie direkt zugewiesen wurde. Weitere Informationen über Richtlinienvererbung finden Sie unter „Netzwerkobjekten Richtlinien zuweisen“ (S. 70).

Gruppen löschen

Eine Gruppe kann nicht gelöscht werden, wenn Sie mindestens einen Endpunkt enthält. Verschieben Sie alle Endpunkte aus der zu löschenden Gruppe in eine andere Gruppe. Wenn die Gruppe Untergruppen enthält, können Sie anstelle von einzelnen Endpunkten auch alle Untergruppen verschieben.

Um eine Gruppe zu löschen:

1. Klicken Sie auf die leere Gruppe im linken Fenster der Seite **Netzwerk**.
2. Klicken Sie auf die Schaltfläche **Gruppe entfernen** im oberen Bereich des linken Fensters. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

4.4. Sortieren, Filtern und Suchen von Endpunkten

Abhängig von der Anzahl der Endpunkte kann sich die Tabelle im rechten Fenster über mehrere Seiten erstrecken (standardmäßig werden nur 20 Einträge pro Seite angezeigt). Verwenden Sie die Navigationsschaltflächen am unteren Rand der Tabelle, um zwischen den Seiten zu wechseln. Um die Anzahl der Einträge zu

ändern, die pro Seite angezeigt werden, wählen Sie die entsprechende Option aus dem Menü neben den Navigationsschaltflächen aus.

Bei zu vielen Einträgen können Sie die Suchfelder unterhalb der Spaltenüberschriften oder das **Filter**-Menü im oberen Bereich der Tabelle verwenden, um nur die Einträge anzuzeigen, die Sie interessieren. So können Sie zum Beispiel nach einem bestimmten Endpunkt suchen oder nur verwaltete Endpunkte anzeigen.

4.4.1. Endpunkte sortieren

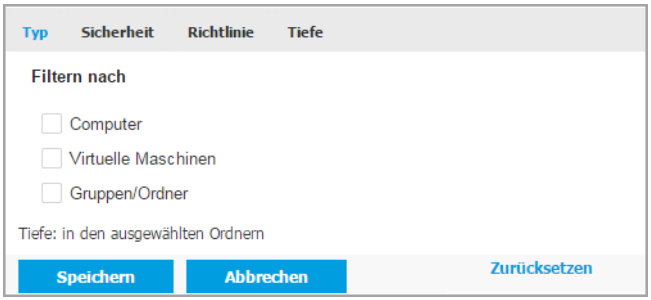
Sie können die Daten in der Tabelle nach dem Inhalt einer bestimmten Spalte sortieren, indem Sie auf die entsprechende Spaltenüberschrift klicken. Wenn Sie zum Beispiel möchten, dass die Endpunkte nach ihrem Namen geordnet werden, klicken Sie auf die Überschrift **Name**. Wenn Sie erneut auf den Titel klicken, werden die Endpunkte in umgekehrter Reihenfolge angezeigt.

Computer sortieren

4.4.2. Endpunkte filtern

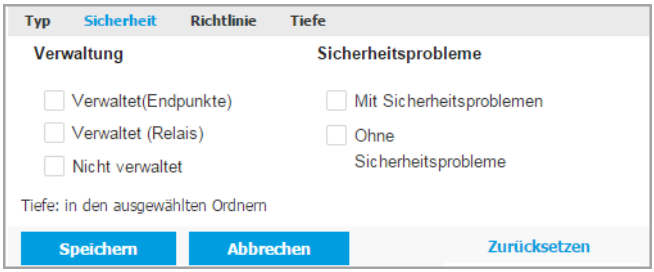
Ihre Netzwerkentitäten können Sie filtern, indem Sie im oberen Bereich der Netzwerkfenster das **Filter**-Menü verwenden.

1. Wählen Sie die gewünschte Gruppe im linken Fenster.
2. Klicken Sie auf das **Filter**-Menü im oberen Bereich der Netzwerkfenster.
3. So verwenden Sie die Filterkriterien:
   - **Typ**. Wählen Sie die Art der Entitäten aus, die angezeigt werden sollen (Computer, virtuelle Maschinen, Ordner).



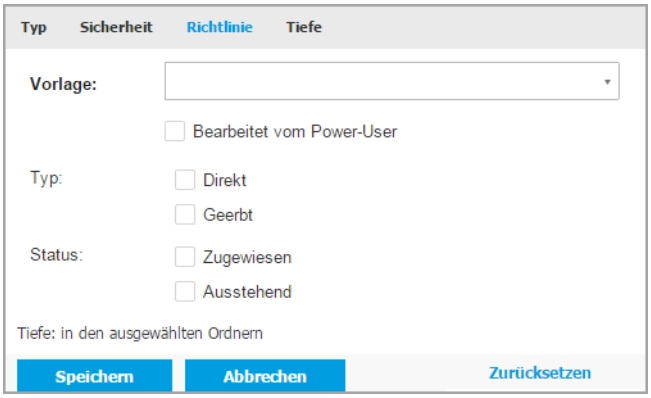
Endpunkte - Nach Typ filtern

- **Sicherheit**. Zeigen Sie Endpunkte nach Verwaltungs- und Sicherheitsstatus an.



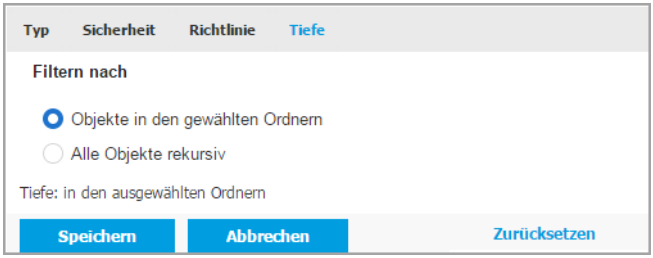
Endpunkte - nach Sicherheit filtern

- **Richtlinie**. Wählen Sie die Richtlinienvorlage, nach der Sie die Endpunkte filtern möchten, den Richtlinienzuweisungstyp (direkt oder geerbt) sowie den Richtlinienzuweisungsstatus (zugewiesen oder ausstehend). Sie können auch nur diejenigen Entitäten anzeigen, die Richtlinien haben, die im Power-User-Modus bearbeitet wurden.



Endpunkte - Nach Richtlinie filtern

- **Tiefe**. Bei der Verwaltung eines Netzwerks mit Baumstruktur werden Endpunkte, die sich in Untergruppen befinden, bei Auswahl der Stammgruppe nicht angezeigt. Wählen Sie **Alle Objekte rekursiv**, um alle Endpunkte der aktuellen Gruppe und alle ihre Untergruppen anzuzeigen.



Endpunkte - Nach Tiefe filtern

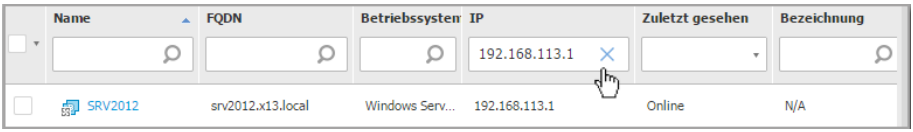
Beachten Sie
Die ausgewählten Filterkriterien werden im unteren Teil des **Filter**-Fensters angezeigt.
Klicken Sie auf **Zurücksetzen**, um alle Filter zu löschen.

4. Klicken Sie auf **Speichern**, um die Endpunkte nach den gewählten Kriterien zu filtern. Der Filter bleibt aktiv in der **Netzwerk**-Übersicht, bis Sie sich abmelden oder den Filter löschen.

4.4.3. Nach Endpunkten suchen

1. Wählen Sie die gewünschte Gruppe im linken Fenster.
2. Geben Sie den Suchbegriff in das entsprechende Feld unter der Spaltenüberschrift im rechten Fenster rein. Geben Sie zum Beispiel die IP-Adresse des Endpunktes, den Sie suchen, in das Feld **IP** ein. Nur der passende Endpunkt wird in der Tabelle angezeigt.

   Leeren Sie das Suchfeld, um die vollständige Liste der Endpunkte anzuzeigen.



Nach Endpunkten suchen

4.5. Aufgaben ausführen

Über die Seite **Netzwerk** können Sie per Fernzugriff eine Reihe administrativer Aufgaben auf Endpunkten ausführen.

Sie haben die folgenden Möglichkeiten:

- „Scan“ (S. 39)
- „Installieren“ (S. 48)
- „Client Deinstallieren“ (S. 52)
- „Client aktualisieren“ (S. 53)
- „Client neu konfigurieren “ (S. 53)
- „Client neu starten“ (S. 55)
- „Netzwerkerkennung“ (S. 55)

Sie können Aufgaben individuell für einzelne Endpunkte oder für Gruppen von Endpunkten erstellen. Sie können zum Beispiel per Ferninstallation den Sicherheitsagenten auf einer Gruppe nicht verwalteter Endpunkte installieren. Später können Sie eine Scan-Aufgabe für einen bestimmten Endpunkt aus dieser Gruppe erstellen.

Auf jedem Endpunkt können Sie nur kompatible Aufgaben ausführen. Wenn Sie zum Beispiel einen nicht verwalteten Endpunkt auswählen, können Sie nur den Sicherheitsagenten installieren; alle anderen Aufgaben sind nicht verfügbar.

Bei einer Gruppe wird die ausgewählte Aufgabe nur für kompatible Endpunkte erstellt. Wenn kein Endpunkt der Gruppe mit der ausgewählten Aufgabe kompatibel ist, werden Sie benachrichtigt, dass die Aufgabe nicht erstellt werden konnte.

Sofort nach der Erstellung startet die Aufgabe auf Endpunkten, die online sind. Wenn ein Endpunkt offline ist, wird die Aufgabe ausgeführt, sobald er wieder online ist.

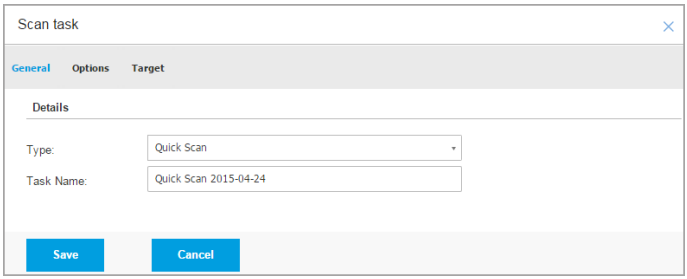
Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten. Weitere Informationen finden Sie unter Aufgaben anzeigen und verwalten.

4.5.1. Scan

So führen Sie eine Scan-Aufgabe per Fernzugriff auf einem oder mehreren Endpunkten aus:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie den gewünschten Container im linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen der Endpunkte oder Gruppen, die Sie scannen möchten.
4. Klicken Sie auf die Schaltfläche **Aufgabe** am oberen Rand der der Tabelle, und wählen Sie **Scan**.

   Ein Konfigurationsfenster wird sich öffnen.
5. Konfigurieren Sie die Scan-Optionen:
   - Im Reiter **Allgemein** können Sie den Scan-Typ auswählen und der Scan-Aufgabe einen Namen geben. Der Name dient nur dazu, dass Sie den Scan auf der Seite **Aufgaben** leicht wiederfinden.



Scan-Aufgabe - Konfigurieren der allgemeinen Einstellungen

Wählen Sie den gewünschten Typ aus dem Menü **Typ**:

- **Quick Scan** setzt auf In-the-Cloud-Scans, um auf Ihrem System laufende Malware aufzuspüren. Dieser Scan ist so vorkonfiguriert, dass nur kritische Windows- und Linux-System-Speicherorte gescannt werden können. Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenscan in Anspruch nehmen würde.

  > **Beachten Sie**
  >
  > Quick Scan findet bestehende Malware, ohne aber irgeneine Aktion auszuführen. Wenn während eines Quick Scan Malware gefunden wird, müssen Sie eine Vollständiger-Scan-Aufgabe ausführen, um die gefundene Malware zu entfernen

- Der **Vollständige Scan** durchsucht das gesamte System nach allen Typen von Malware, die ein Sicherheitsrisiko darstellen, so z. B. Viren, Spyware, Adware, Rootkits usw.
- **Speicher-Scan** überprüft die Programme, die im Speicher des Endpunktes laufen.
- **Netzwerk-Scan** ist ein benutzerdefinierter Scan, mit dem Netzwerklaufwerke mit dem Bitdefender-Sicherheitsagenten, der auf dem ansprechenden Endpunkt installiert ist, gescannt werden können.

  Damit die Netzwerk-Scan-Aufgabe funktioniert, müssen folgende Voraussetzungen erfüllt sein:

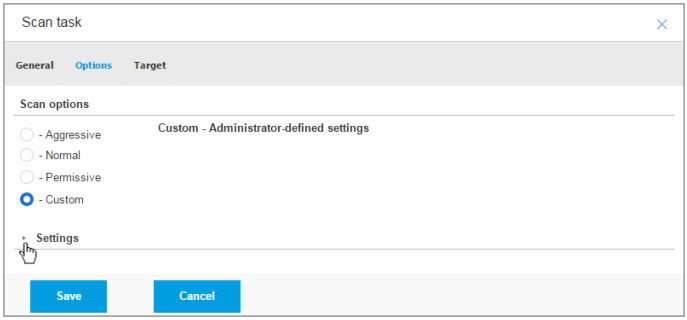
- Sie müssen die Aufgabe einem einzelnen Endpunkt in Ihrem Netzwerk zuweisen.
- Sie müssen die Zugangsdaten eines Benutzerkontos mit Lese- und Schreibberechtigung auf den entsprechenden Netzwerklaufwerken eingeben, damit der Sicherheitsagent auf diese Netzwerklaufwerke zugreifen und die entsprechenden Aktionen durchführen kann. Die nötigen Zugangsdaten können Sie im Aufgabenfenster im Reiter **Ziel** konfigurieren.

– **Benutzerdefinierter Scan** Hierbei können Sie die Bereiche, die gescannt werden sollen, selbst auswählen und die Scan-Optionen festlegen.

Für benutzerdefinierte Scans müssen Sie die folgenden Einstellungen konfigurieren:

– Gehen Sie zum Reiter **Optionen**, um die Scan-Optionen festzulegen. Klicken Sie auf die Sicherheitsstufe, die Ihren Ansprüchen entspricht (aggressiv, normal oder tolerant). Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.

  Je nach ausgewähltem Profil werden die Scan-Optionen im Bereich **Einstellungen** automatisch konfiguriert. Bei Bedarf können Sie diese aber auch im Detail konfigurieren. Markieren Sie dazu das Kästchen **Benutzerdefiniert** und vergrößern Sie dann den Bereich **Einstellungen**.



Scan-Aufgabe - Konfiguration eines benutzerdefinierten Scans

Die folgenden Optionen sind verfügbar:

- **Dateitypen.** Verwenden Sie diese Optionen, um festzulegen, welche Dateien gescannt werden sollen. Sie können den Sicherheitsagenten

so einrichten, dass Scans entweder für alle Dateien (unabhängig von der Dateiendung), oder nur für Anwendungsdateien oder nur für bestimmte Dateiendungen, die Sie für gefährlich erachten, durchgeführt werden. Das Scannen aller Dateien bietet den besten Schutz, während das Scannen nur von Anwendungen verwendet wird, um einen schnelleren Scan durchzuführen.

Beachten Sie

Anwendungsdateien sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen. Weitere Informationen finden Sie unter „Anwendungsdateitypen“ (S. 176).

Wenn Sie nur bestimmte Dateiendungen scannen lassen möchten, wählen Sie **Benutzerdefinierte Endungen** aus dem Menü, und geben Sie dann die Endungen in das Eingabefeld ein. Klicken Sie nach jeder Eingabe auf `Speichern`.

Wichtig

Bitdefender-Sicherheitsagenten, die auf Windows- und Linux-Systemen installiert sind, scannen die meisten ISO-Formate, führen aber keine Aktionen für sie durch.

Optionen für eine Scan-Aufgabe - Hinzufügen von benutzerdefinierten Endungen

- **Archive.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für die Systemsicherheit. Die Malware kann das System nur beeinflussen, wenn die infizierten Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird. Wir empfehlen jedoch, Archive zu scannen, um jegliche potentiellen Bedrohungen aufzuspüren und zu entfernen, auch wenn es sich nicht um unmittelbare Bedrohungen handelt.

Wichtig
Das Scannen archivierter Dateien erhöht die Gesamt-Scandauer und erfordert mehr Systemressourcen.

- **Inhalt von Archiven scannen.** Wählen Sie diese Option, wenn Sie archivierte Dateien nach Malware durchsuchen möchten. Sollten Sie sich zur Verwendung dieser Option entscheiden, können Sie die folgenden Optimierungsoptionen konfigurieren:
  - **Archivgröße begrenzen auf (MB).** Sie können Sie die maximale Größe der Archive angeben, die gescannt werden sollen. Markieren Sie das entsprechende Kästchen und geben Sie die maximale Archivgröße in MB ein.
  - **Maximale Archivtiefe (Ebenen).** Markieren Sie das entsprechende Kästchen und wählen Sie die maximale Archivtiefe aus dem Menü. Für optimale Leistung wählen Sie den niedrigsten Wert, für maximalen Schutz wählen Sie den höchsten Wert.
- **E-Mail-Archive scannen.** Wählen Sie diese Option, wenn Sie möchten, dass E-Mail-Dateien und E-Mail-Datenbanken (Dateiformate wie EML, MSG, PST, DBX, MBX, TBB usw.) gescannt werden.

  Wichtig
  Das Scannen von E-Mail-Archiven kann viele Ressourcen beansprucht und die Systemleistung beeinträchtigen.

- **Verschiedenes.** Markieren Sie die entsprechenden Kästchen, um die gewünschten Scan-Optionen zu aktivieren.
  - **Boot-Sektoren scannen.** Prüft die Bootsektoren des Systems. Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten. Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.
  - **Registry scannen.** Wählen Sie diese Option, um die Registry-Schlüssel zu scannen. Die Windows-Registry ist eine Datenbank, in der Konfigurationseinstellungen und Optionen für

die Windows-Betriebssystemkomponenten sowie für die installierten Anwendungen gespeichert sind.

- **Nach Rootkits suchen.** Wählen Sie diese Option, um nach Rootkits und Objekten zu suchen, die mit dieser Art von Software versteckt werden.
- **Nach Keyloggern suchen.** Wählen Sie diese Option, wenn nach Keylogger-Software gesucht werden soll.
- **Speicher scannen.** Wählen Sie diese Option, um Programme zu scannen, die im Speicher des Systems laufen.
- **Cookies scannen.** Wählen Sie diese Option, um die Cookies zu scannen, die von Ihrem Browser auf dem Computer gespeichert werden.
- **Nur neue und geänderte Dateien.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Nach potenziell unerwünschten Anwendungen (PUA) scannen.** Eine potenziell unerwünschte Anwendung (PUA) ist ein Programm, das auf dem PC vermutlich nicht erwünscht ist und häufig in Verbindung mit Freeware installiert wurde. Diese Art von Programmen kann ohne Zustimmung des Benutzers installiert werden (wird auch als Adware bezeichnet) oder wird standardmäßig bei der Express-Installation mitinstalliert (werbeunterstützt). Diese Programme können Pop-up-Werbung anzeigen, unerwünschte Symbolleisten im Standard-Browser installieren oder Hintergrundprozesse ausführen und so den PC verlangsamen.
- **Wechseldatenträger scannen.** Wählen Sie diese Option, um Wechseldatenträger zu scannen, die mit dem Endpunkt verbunden sind.

- **Aktionen.** Abhängig vom gefundenen Dateityp werden folgende Aktionen automatisch ausgeführt:
  - **Wenn eine infizierte Datei gefunden wird.** Als infiziert eingestufte Dateien stimmen mit einer Malware-Signatur der Bitdefender Malware-Signaturen-Datenbank überein. Der

Bitdefender-Sicherheitsagent kann normalerweise den Malware-Code aus einer infizierten Datei entfernen und die ursprüngliche Datei rekonstruieren. Diesen Vorgang bezeichnet man als Desinfektion.

Wenn eine infizierte Datei gefunden wird, versucht der Bitdefender-Sicherheitsagent automatisch, diese zu desinfizieren. Falls die Desinfizierung fehlschlägt, wird die Datei in die Quarantäne verschoben, um dort die Infizierung einzudämmen.

Wichtig
Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- **Wenn eine verdächtige Datei gefunden wird.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert. Da es sich bei B-HAVE um eine heuristische Analysetechnologie handelt, kann Endpoint Security nicht sicher sein, ob die Datei tatsächlich mit Malware infiziert ist. Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.

  Scan-Aufgaben sind standardmäßig so konfiguriert, dass verdächtigte Dateien ignoriert werden. Es könnte ratsam sein, die Standardaktion zu ändern, damit verdächtige Dateien in Quarantäne verschoben werden. Dateien in Quarantäne werden zu Analysezwecken in regelmäßigen Abständen an die Bitdefender-Labs geschickt. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

- **Wenn ein Rootkit gefunden wurde.** Rootkits sind spezielle Software-Wekzeuge, die verwendet werden, um Dateien vor dem Betriebssystem zu verbergen. Obwohl sie nicht zwangsläufig als schädlich anzusehen sind, werden Rootkits häufig genutzt, um Malware zu verbergen oder Eindringlinge im System zu tarnen.

  Erkannte Rootkits und versteckte Dateien werden standardmäßig ignoriert.

Sie können die standardmäßigen Aktionen verändern, dies wird aber nicht empfohlen. Sie können eine zweite Aktion auswählen, für den Fall, dass die Erste fehlschlägt und außerdem verschiedene Aktionen für jede Kategorie. Wählen Sie aus den entsprechenden Menus die erste und zweite Aktion, die für jeden entdeckten Dateityp vorgenommen werden soll. Folgende Aktionen stehen zur Verfügung:

Desinfizieren
Den Malware-Kode aus den entdeckten infizierten Dateien entfernen. Es wird empfohlen, dass dies immer die erste Aktion bleibt, die für infizierte Dateien durchgeführt wird.

Dateien in Quarantäne verschieben
Verschieben Sie infizierte Dateien von ihrem Speicherort in den Quarantäne-Ordner. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. Sie können die Dateien in Quarantäne über die Quarantäne-Seite in der Konsole verwalten.

Löschen
Infizierte Dateien ohne vorherige Benachrichtigung von der Festplatte löschen. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.

Ignorieren
Für gefundene Dateien wird keine Aktion durchgeführt. Diese Dateien werden nur in das Scan-Protokoll aufgenommen.

– Gehen Sie zum Reiter **Ziel**, um die Speicherorte konfigurieren, die auf den Ziel-Endpunkten gescannt werden sollen.

Im Bereich **Scan-Ziel** können Sie eine neue Datei oder einen neuen Ordner hinzufügen, die/der gescannt werden soll:

a. Wählen Sie einen vorgegebenen Speicherort aus dem Klappmenü, oder geben Sie **Bestimmte Pfade** ein, die sie scann lassen möchten.

b. Geben Sie den Pfad des zu scannenden Objekts im Bearbeitungsfeld ein.

- Wenn Sie einen vorgegebenen Pfad ausgewählt haben, vervollständigen Sie den Pfad nach Bedarf. Um zum Beispiel den gesamten Ordner `Programme` zu scannen, müssen Sie lediglich den entsprechenden vorgegebenen Pfad aus dem Klappmenü

auswählen. Um einen bestimmten Order im Ordner `Programme` zu scannen, müssen Sie den Pfad vervollständigen indem Sie einen Backslash (\) und den Namen des Ordners hinzufügen.

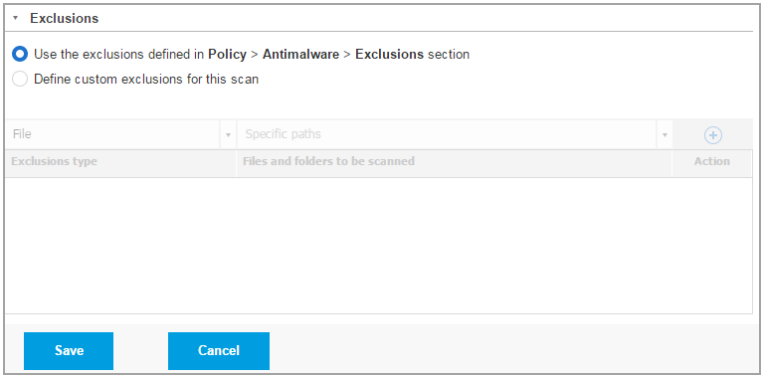
- Wenn Sie **Bestimmte Pfade** ausgewählt haben, geben Sie den vollständigen Pfad des Objektes ein, das gescannt werden soll. Es empfiehlt sich, (nach Möglichkeit) Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist. Weitere Informationen zu den Systemvariablen finden Sie unter „Systemvariablen“ (S. 177).

c. Klicken Sie auf den entsprechenden ⊕ **Hinzufügen**-Link.

Um einen bestehenden Pfad zu bearbeiten, klicken Sie ihn an. Um einen Pfad aus der Liste zu löschen, klicken Sie auf die entsprechende ⊗ **Löschen**-Schaltfläche.

Für Netzwerk-Scan-Aufgaben müssen Sie die Zugangsdaten eines Benutzerkontos mit Lese- und Schreibberechtigung auf den entsprechenden Netzwerklaufwerken eingeben, damit der Sicherheitsagent auf diese Netzwerklaufwerke zugreifen und die entsprechenden Aktionen durchführen kann.

Klicken Sie auf die Bereiche **Ausschlüsse**, wenn Sie bestimmte Ziele vom Scan ausschließen möchten.



Scan-Aufgabe - Definieren von Ausschlüssen

Sie können entweder die per Richtlinie definierten Ausschlüsse verwenden oder für die aktuelle Scan-Aufgabe bestimmte Ausschlüsse definieren. Weitere Informationen finden Sie unter „Ausschlüsse“ (S. 101).

6. Klicken Sie auf **Speichern**, um die Scan-Aufgabe zu erstellen. Eine Bestätigungsmeldung wird angezeigt.
7. Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter Aufgaben anzeigen und verwalten.

4.5.2. Installieren

Um Ihre Endpunkte zu schützen, müssen Sie auf jedem von ihnen den Bitdefender-Sicherheitsagenten installieren.

Sobald Sie einen Relais-Agenten installiert haben, findet dieser automatisch ungeschützte Endpunkte im selben Netzwerk.

Die Bitdefender-Sicherheitssoftware kann per Fernzugriff über das Control Center auf Endpunkten installiert werden.

Die Remote-Installation erfolgt im Hintergrund, ohne dass der Benutzer dies bemerkt.

Warnung

Vor der Installation sollten Sie bereits installierte Malware-Schutz- und Firewall-Software deinstallieren. Wenn die Bitdefender-Sicherheitssoftware über bestehende Sicherheitssoftware installiert wird, kann dies die jeweilige Funktion stören und massive Probleme auf dem System verursachen. Windows Defender und die Windows-Firewall werden beim Start der Installation automatisch deaktiviert.

So führen Sie eine Ferninstallationsaufgabe aus:

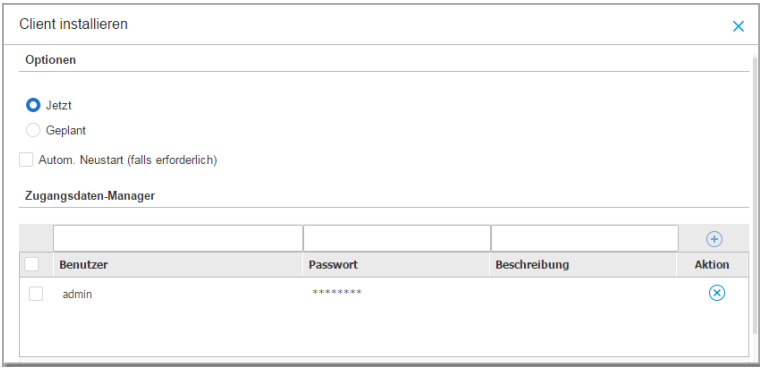
1. Stellen Sie eine Verbindung zur Control Center her und melden Sie sich an.
2. Gehen Sie zur Seite **Netzwerk**.
3. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Die Entitäten der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.

Beachten Sie

Sie können optional auch Filter anwenden, um ausschließlich die nicht verwalteten Endpunkte anzuzeigen. Klicken Sie auf das **Filter**-Menü und wählen Sie die folgenden Optionen: **Nicht verwaltet** aus dem Reiter **Sicherheit** und **Alle Objekte rekursiv** aus dem Reiter **Tiefe**.

4. Wählen Sie die Entitäten (Endpunkte oder Gruppen von Endpunkten) aus, auf denen Sie den Schutz installieren möchten.
5. Klicken Sie auf die Schaltfläche **Aufgaben** am oberen Rand der der Tabelle, und wählen Sie **Installieren**.

   Der Assistent **Client installieren** wird angezeigt.



Installation von Bitdefender Endpoint Security Tools über das Aufgabenmenü

6. Konfigurieren Sie im Bereich **Optionen** den Installationszeitpunkt:
   - **Jetzt** - hiermit startet die Installation sofort.
   - **Geplant** - hiermit legen Sie ein Intervall für die Wiederholung der Installation fest. Wählen Sie einfach das Intervall (stündlich, täglich oder wöchentlich), das Ihnen am besten passt.

     Beachten Sie

     Wenn zum Beispiel bestimmte Operationen auf einer bestimmten Maschine nötig sind, bevor der Client installiert wird (z. B. Deinstallation anderer Software oder Neustart des Betriebssystems), können Sie die Installationsaufgabe für alle 2 Stunden planen. Die Aufgabe wird dann auf jeder entsprechenden Maschine alle 2 Stunden ausgeführt, bis die gesamte Installation abgeschlossen ist.

7. Wenn Sie möchten, dass die Endpunkte nach Abschluss der Installation automatisch neu gestartet werden, wählen Sie **Autom. Neustart (falls erforderlich)**.

8. Geben Sie im Bereich **Zugangsdaten-Manager** die Administratorzugangsdaten an, die für die Fernauthentifizierung auf den entsprechenden Endpunkten benötigt werden. Sie können die Zugangsdaten hinzufügen, indem Sie den Benutzer und das Passwort der Zielbetriebssysteme eingeben.

   Wichtig
   Bei Windows-8.1-Systemen müssen Sie die Zugangsdaten des eingebauten Administratorkontos oder die eines Domänenadministratorkontos eingeben. Weiteres zu diesem Thema erfahren Sie in diesem Artikel.

   So fügen Sie erforderlichen OS-Zugangsdaten hinzu:

   a. Geben Sie im entsprechenden Feld in der Spaltenüberschrift den Benutzernamen und das Passwort eines Administratorkontos ein.

      Wenn Computer in einer Domäne sind, reicht es aus, die Anmeldeinformationen des Domänenadministrators einzugeben.

      Verwenden Sie Windows-Konventionen, wenn Sie den Namen eines Domain-Benutzerkontos eingeben, z. B. `user@domain.com` oder `domain\user`). Um sicherzugehen, dass die eingegebenen Zugangsdaten funktionieren, geben Sie sie in beiden Ausdrucksweisen ein (`user@domain.com` und `domain\user`).

      Sie können jedem Konto eine Beschreibung hinzufügen, um es später leichter identifizieren zu können.

   b. Klicken Sie auf den Button ⊕**Hinzufügen**. Das Konto wird zu der Liste der Zugangsdaten hinzugefügt.

      Beachten Sie
      Die angegebenen Zugangsdaten werden automatisch im Zugangsdaten-Manager gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben müssen. Den Zugangsdaten-Manager können Sie einfach öffnen, indem Sie mit dem Mauszeiger auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole fahren.

      Wichtig
      Sind die für einen Endpunkt eingegebenen Zugangsdaten ungültig, schlägt die Installation des Clients auf diesem Endpunkt fehl. Denken Sie daran, die eingegebenen Zugangsdaten im Zugangsdaten-Manager zu aktualisieren, wenn sie auf den Endpunkten geändert werden.

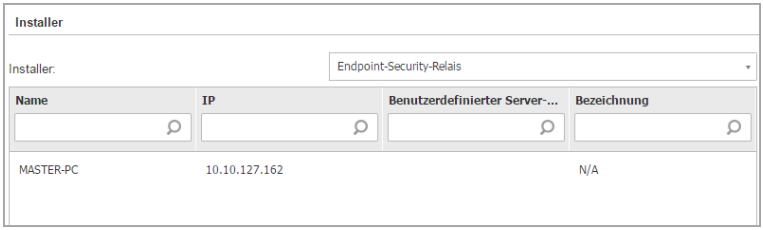
9. Markieren Sie die Kästchen für die Konten, die Sie verwenden möchten.

   Beachten Sie
   Wenn Sie noch keine Zugangsdaten ausgewählt haben, wird eine Warnmeldung angezeigt. Dieser Schritt kann bei der Ferninstallation des Sicherheitsagenten auf Endpunkten nicht ausgelassen werden.

10. Konfigurieren Sie im Bereich **Installer** das Relais, zu dem die Endpunkte eine Verbindung herstellen sollen, um den Client zu installieren und zu aktualisieren:

    - Alle Maschinen mit der Relais-Rolle, die in Ihrem Netzwerk gefunden wurden, werden in der Tabelle im Bereich **Installer** aufgeführt. Jeder neue Client muss mit mindestens einem Relais-Client desselben Netzwerks verbunden sein, der als Kommunikations- und Update-Server fungiert. Wählen Sie das Relais, das Sie mit den gewünschten Endpunkten verknüpfen möchten. Verbundene Endpunkte kommunizieren mit dem Control Center ausschließlich über das angegebene Relais.

      Wichtig
      Port 7074 muss offen sein, damit die Installation über einen Relais-Agenten funktioniert.

    - Wenn die gewünschten Endpunkte über einen Proxy mit dem Relais-Agenten kommunizieren, müssen Sie auch die Proxy-Einstellungen definieren. Wählen Sie in diesem Fall **Proxy für die Kommunikation verwenden** und geben Sie die nötigen Proxy-Einstellungen in de entsprechenden Felder ein.

11. Sie müssen ein Installationspaket für die aktuelle Installation auswählen. Klicken Sie auf die Liste **Paket verwenden** und wählen Sie das gewünschte Paket. Hier finden Sie alle bisher für Ihr Konto erstellten Installationspakete ebenso wie das Standard-Installationspaket, das im Control Center enthalten ist.

12. Wenn nötig, können Sie die Einstellungen des ausgewählten Installationspakets abändern, indem Sie neben dem Feld **Paket verwenden** auf die Schaltfläche **Anpassen** klicken.

    Die Einstellung des Installationspakets werden unten angezeigt, und Sie können die nötigen Änderungen vornehmen. Weitere Informationen zur Bearbeitung von Installationspaketen finden Sie in der GravityZone-Installationsanleitung.

    Wenn Sie die Änderungen als neues Paket speichern möchten, wählen Sie die Option **Als Paket speichern** unter der Paketeinstellungsliste und vergeben Sie einen neuen Namen für das neue Paket.

13. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.

Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten.

4.5.3. Client Deinstallieren

So entfernen Sie die Bitdefender-Sicherheitssoftware per Fernzugriff:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie den gewünschten Container im linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen der Endpunkte, von denen Sie den Bitdefender-Sicherheitsagenten deinstallieren möchten.
4. Klicken Sie auf die Schaltfläche **Aufgabe** am oberen Rand der Tabelle, und wählen Sie **Client deinstallieren**.
5. Ein Konfigurationsfenster wird angezeigt, in dem Sie sich für den Verbleib Quarantäne-Objekte auf der Client-Maschine entscheiden können.
6. Klicken Sie auf **Speichern**, um die Aufgabe zu erstellen. Eine Bestätigungsmeldung wird angezeigt.

   Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter Aufgaben anzeigen und verwalten.

Beachten Sie
Wenn Sie den Schutz erneut installieren möchten, müssen Sie den Computer zuerst neu starten.

4.5.4. Client aktualisieren

Überprüfen Sie den Status verwalteter Computer in regelmäßigen Abständen. Wenn Ihnen ein Computer mit Sicherheitsproblemen auffällt, klicken Sie auf seinen Namen, um die Seite **Informationen** anzuzeigen. Weitere Informationen finden Sie unter „Endpunktsicherheitsstatus“ (S. 28).

Veraltete Clients oder Signaturen stellen Sicherheitsprobleme dar. In diesen Fälle sollten Sie ein Update auf dem entsprechenden Computer durchführen. Diese Aufgabe kann lokal vom Computer aus oder per Fernzugriff von der Control Center aus durchgeführt werden.

So können Sie den Client und die Signaturen auf verwalteten Computern per Fernzugriff aktualisieren:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie den gewünschten Container im linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen der Endpunkte, auf denen Sie ein Client-Update durchführen möchten.
4. Klicken Sie auf die Schaltfläche **Aufgabe** am oberen Rand der der Tabelle, und wählen Sie **Update**. Ein Konfigurationsfenster wird sich öffnen.
5. Sie können nach Belieben nur das Produkt, nur die Virensignaturen oder beides aktualisieren.
6. Klicken Sie auf **Update**, um die Aufgabe auszuführen. Eine Bestätigungsmeldung wird angezeigt.

   Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter Aufgaben anzeigen und verwalten.

4.5.5. Client neu konfigurieren

Die Module, Rollen und Scan-Modi des Sicherheitsagenten sind zunächst im Installationspaket konfiguriert. Nach der Installation des Sicherheitsagenten in Ihrem Netzwerk können Sie die anfänglichen Einstellungen jederzeit ändern, indem Sie per Fernzugriff einer Aufgabe **Client neu konfigurieren** an die gewünschten verwalteten Endpunkte senden.

Warnung
Bitte beachten Sie, dass die Aufgabe **Client neu konfigurieren** alle Installationseinstellungen überschreibt. Keine der ursprünglich Einstellungen wird beibehalten. Achten Sie bei der Verwendung dieser Aufgabe darauf, alle Installationseinstellungen für die gewünschten Endpunkte neu zu konfigurieren.

So ändern Sie die Installationseinstellungen für einen oder mehrere Endpunkte:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen der Endpunkte, bei denen Sie die Installationseinstellungen ändern möchten.
4. Klicken Sie auf die Schaltfläche **Aufgabe** am oberen Rand der Tabelle, und wählen Sie **Client neu konfigurieren**.
5. Konfigurieren Sie im Bereich **Allgemein** den Zeitpunkt, zu dem die Aufgabe ausgeführt werden soll:
   - **Jetzt** - hiermit startet die Aufgabe sofort.
   - **Geplant** - hiermit legen Sie ein Intervall für die Wiederholung der Aufgabe fest. Wählen Sie einfach das Intervall (stündlich, täglich oder wöchentlich), das Ihnen am besten passt.

     Beachten Sie
     Wenn zum Beispiel andere wichtige Prozesse ebenfalls auf der Maschine ausgeführt werden müssen, können Sie die Aufgabe so planen, dass sie alle 2 Stunden ausgeführt wird. Die Aufgabe wird dann auf jeder entsprechenden Maschine alle 2 Stunden ausgeführt, bis sie erfolgreich abgeschlossen wird.

6. Konfigurieren Sie die Module, Rollen und Scan-Modi für die gewünschten Endpunkte nach Bedarf. Weitere Informationen hierzu finden Sie in der GravityZone-Installationsanleitung.

   Warnung
   Es werden nur die Module installiert, die vom jeweiligen Betriebssystem unterstützt werden.
   Bitte beachten Sie, dass das Firewall-Modul steht nur für Windows-Arbeitsplätze zur Verfügung.

7. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.

   Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter Aufgaben anzeigen und verwalten.

4.5.6. Client neu starten

Sie können verwaltete Endpunkte aus der Ferne neu starten.

Beachten Sie
Bevor Sie einzelne Endpunkte neu starten, sollten Sie einen Blick auf die Seite **Netzwerk > Aufgaben** werfen. Zuvor erstellte Aufgaben könnten derzeit noch auf den ausgewählten Endpunkten laufen.

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie den gewünschten Container im linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen der Endpunkte, die Sie neu starten möchten.
4. Klicken Sie auf die Schaltfläche **Aufgabe** am oberen Rand der Tabelle, und wählen Sie **Client neu starten**.
5. Wählen Sie den Zeitpunkt des Neustarts:
   - Wählen Sie **Jetzt neu starten**, um die Endpunkte sofort neu zu starten.
   - Wählen Sie **Neustadt am**, und nutzen Sie die Eingabefelder weiter unten, um den Neustart für einen beliebigen Zeitraum zu planen.
6. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.

   Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter Aufgaben anzeigen und verwalten.

4.5.7. Netzwerkerkennung

Die Netzwerkerkennung wird automatisch stündlich von Sicherheitsagenten mit Relais-Rolle durchgeführt. Sie können aber auch jederzeit manuell eine Netzwerkerkennungsaufgabe über das Control Center einer beliebigen durch einen Relais-Agenten geschützten Maschine durchführen.

So führen Sie eine Netzwerkerkennungsaufgabe in Ihrem Netzwerk durch:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie den gewünschten Container im linken Fenster. Alle Endpunkte des ausgewählten Containers werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen des Relais-Endpunktes, über den Sie eine Netzwerkerkennung durchführen möchten.
4. Klicken Sie auf die Schaltfläche **Aufgabe** am oberen Rand der Tabelle, und wählen Sie **Netzwerkerkennung**.
5. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **Ja**.

   Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter Aufgaben anzeigen und verwalten.

4.6. Schnellberichte erstellen

Auf der Seite **Netzwerk** können Sie Sofortberichte zu verwalteten Endpunkten erstellen:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Alle Endpunkte der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.

   Wenn Sie möchten, können Sie den Inhalt der ausgewählten Gruppe nur nach verwalteten Endpunkten filtern.
3. Markieren Sie die Kästchen der Computer, die im Bericht enthalten sein sollen.
4. Klicken Sie auf die Schaltfläche **Bericht** am oberen Rand der Tabelle, und wählen Sie den Berichtstyp aus dem Menü.

   Weitere Informationen finden Sie unter „Verfügbare Berichtstypen“ (S. 140).
5. Konfigurieren Sie die Berichtsoptionen. Weitere Informationen finden Sie unter „Berichte erstellen“ (S. 144).
6. Klicken Sie auf **Generieren**. Der Bericht wird sofort angezeigt.

   Es dauert unterschiedlich lange, bis Berichte erstellt sind, je nach Anzahl der gewählten Endpunkte.

4.7. Richtlinien zuweisen

Über Richtlinien können Sie Sicherheitseinstellungen auf Endpunkten verwalten.

Auf der Seite **Netzwerk** können Sie Richtlinien für jeden Endpunkt bzw. jede Gruppe von Endpunkten anzeigen, ändern und zuweisen.

Beachten Sie
Sicherheitseinstellungen stehen nur für verwaltete Endpunkte zur Verfügung. Um Sicherheitseinstellungen leichter überblicken und verwalten zu können, können Sie das Netzwerkinventar auch nach verwalteten Endpunkten Filtern.

So zeigen Sie die Richtlinie an, die einem bestimmten Endpunkt zugewiesen wurde:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Alle Endpunkte der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
3. Klicken Sie auf den Namen des verwalteten Endpunktes, der Sie interessiert. Es öffnet sich ein Informationsfenster.
4. Klicken Sie im Reiter **Allgemein** des Bereichs **Richtlinie** auf den Namen der aktuellen Richtlinie, um ihre Einstellungen anzuzeigen.
5. Sie können die Sicherheitseinstellungen nach Bedarf ändern, sofern der Richtlinienersteller Änderungen an dieser Richtlinie durch andere Benutzer erlaubt hat. Bitte beachten Sie, dass Ihre Änderungen sich auch auf alle anderen Endpunkte auswirken, denen diese Richtlinie zugewiesen wurde.

   Weitere Informationen zur Änderung von Richtlinieneinstellungen finden Sie unter „Richtlinien für Computer und virtuelle Maschinen“ (S. 72).

So weisen Sie einem Computer oder einer Gruppe eine Richtlinie zu:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Alle Endpunkte der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie das Kästchen des gewünschten Endpunkts bzw. der gewünschten Gruppe. Sie können auch mehrere Objekte auswählen, diese müssen dann jedoch Objekte desselben Typs und von derselben Ebene sein.
4. Klicken Sie auf die Schaltfläche **Richtlinie zuweisen** am oberen Ende der Tabelle.
5. Nehmen Sie im Fenster **Richtlinienzuweisung** die nötigen Einstellungen vor. Weitere Informationen finden Sie unter „Netzwerkobjekten Richtlinien zuweisen“ (S. 70).

4.8. Endpunkte aus dem Netzwerkinventar löschen

Das Netzwerkinventar enthält standardmäßig den Ordner **Gelöscht**, in dem Endpunkte gespeichert sind, die Sie nicht verwalten möchten.

Wenn Sie die Aktion **Löschen** für einen Endpunkt ausführen, wird er in den Ordner **Gelöscht** verschoben.

So löschen Sie Endpunkte aus dem Netzwerkinventar:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie im linken Fenster die gewünschte Netzwerkgruppe.
3. Markieren Sie im rechten Fenster das Kästchen für den zu löschenden Endpunkt.
4. Klicken Sie auf die Schaltfläche ⊖ **Löschen** am oberen Rand der Tabelle. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

   Der Endpunkt wird in den Ordner **Gelöscht** verschoben.

Sie können Endpunkte aus dem Ordner **Gelöscht** jederzeit mit der Maus nach **Benutzerdefinierte Gruppen** ziehen.

Gelöschte Endpunkte können Sie endgültig aus dem Netzwerkinventar entfernen, indem Sie sie im Ordner **Gelöscht** löschen. Dann werden diese Endpunkte auch aus der GravityZone-Datenbank entfernt.

So entfernen Sie Endpunkte endgültig aus dem Control Center:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die Gruppe **Gelöscht** im linken Fenster. Alle Endpunkte dieser Gruppe werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen der Endpunkte, die Sie endgültig entfernen möchten.
4. Klicken Sie auf die Schaltfläche ⊖ **Löschen** am oberen Rand der Tabelle. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

   Die ausgewählten Endpunkte werden dauerhaft aus der GravityZone-Datenbank entfernt.

   Wenn der endgültig gelöschte Endpunkt verwaltet war, läuft der Sicherheitsagent ab, wodurch ein Arbeitsplatz der Lizenz wieder frei wird.

4.9. Aufgaben anzeigen und verwalten

Auf der Seite **Netzwerk > Aufgaben** können Sie alle Aufgaben, die Sie erstellt haben, einsehen und verwalten.

Sobald Sie eine Aufgabe für Netzwerkobjekte erstellt haben, wird sie in der Aufgabentabelle aufgeführt.

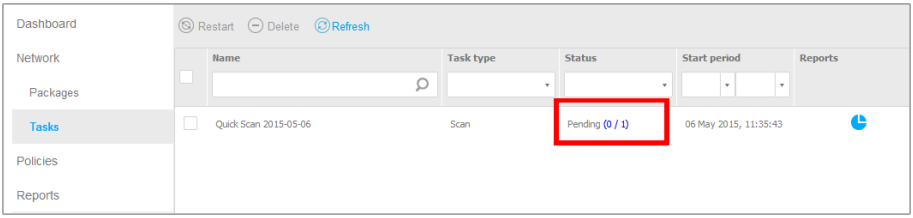
Auf der Seite **Netzwerk > Aufgaben** haben Sie folgende Möglichkeiten:

- Aufgabenstatus überprüfen
- Aufgabenberichte anzeigen
- Aufgaben erneut ausführen
- Aufgaben löschen

4.9.1. Aufgabenstatus überprüfen

Wenn Sie eine Aufgabe für Netzwerkobjekte erstellen, werden Sie den Fortschritt der Aufgabe überprüfen wollen und benachrichtigt werden, wenn Fehler auftreten.

Auf der Seite **Netzwerk > Aufgaben** informiert Sie die Spalte **Status** der einzelnen Aufgaben über den jeweiligen Status. Sie können den Status der Hauptaufgabe überprüfen und detaillierte Informationen über jede Teilaufgabe abrufen.



Die Aufgabenübersicht

- **Status der Hauptaufgabe überprüfen**.

  Die Hauptaufgabe ist die Aktion, die auf die Netzwerkobjekte angewendet wird (wie zum Beispiel Installation des Clients oder Scan). Sie enthält bestimmte Teilaufgaben, eine für jedes Netzwerkobjekt. So enthält eine Installationshauptaufgabe für acht Computer zum Beispiel acht Teilaufgaben. Die Zahlen in Klammern geben an, wie viele Teilaufgaben schon abgeschlossen wurden. So bedeutet (2/8) zum Beispiel, dass zwei von acht Teilaufgaben abgeschlossen sind.

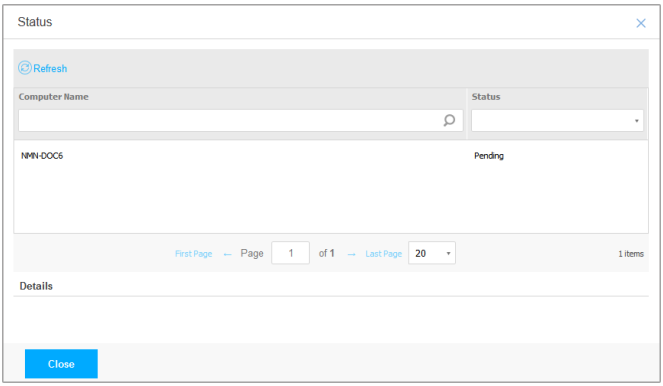
Die Hauptaufgabe kann einen der folgenden Status haben:
- **Ausstehend**, wenn bisher keine der Teilaufgaben gestartet wurde.
- **Wird ausgeführt** - wenn alle Teilaufgaben laufen. Die Hauptaufgabe bleibt in diesem Status, bis die letzte Teilaufgabe abgeschlossen ist.
- **Fertig**, wenn alle Teilaufgaben (erfolgreich oder erfolglos) beendet wurden. Bei erfolglosen Teilaufgaben wird ein Warnsymbol angezeigt.

- **Status der Teilaufgaben überprüfen**.

  Gehen Sie zur Aufgabe, die Sie interessiert, und klicken Sie auf den Link in der Spalte **Status**, um das Fenster **Status** zu öffnen. Dort werden die Netzwerkobjekte, auf die die Hauptaufgabe sich bezieht, sowie der Status jeder Teilaufgabe angezeigt. Die Teilaufgaben können folgende Status haben:

  - **Wird ausgeführt** - wenn die Teilaufgabe noch läuft.
  - **Fertig** - wenn die Teilaufgabe erfolgreich abgeschlossen wurde.
  - **Ausstehend** - wenn die Teilaufgabe noch nicht gestartet wurde. Das kann in den folgenden Situationen passieren:
    - Die Teilaufgabe wartet in einer Warteschlange.
    - Es gibt Verbindungsprobleme zwischen der Control Center und dem Zielobjekt im Netzwerk.
  - **Fehlgeschlagen** - wenn die Teilaufgabe nicht gestartet werden konnte oder wegen eines Fehlers wie ungültigen Zugangsdaten oder zu geringem Speicher angehalten wurde.

  Sie können Details zu einzelnen Teilaufgaben anzeigen, indem Sie sie auswählen und im Bereich **Details** unten in der Tabelle nachsehen.



Aufgabenstatusdetails

Dort finden Sie die folgenden Informationen:

- Datum und Uhrzeit des Aufgabenstarts.
- Datum und Uhrzeit des Aufgabenendes.
- Beschreibung aufgetretener Fehler.

4.9.2. Aufgabenberichte anzeigen

Auf der Seite **Netzwerk > Aufgaben** können Sie Schnellberichte zu Scan-Aufgaben lesen.

1. Gehen Sie zur Seite **Netzwerk > Aufgaben**.
2. Markieren Sie das Kästchen der Scan-Aufgabe, die Sie interessiert.
3. Klicken Sie auf die entsprechende Schaltfläche in der Spalte **Berichte**. Warten Sie, bis der Bericht angezeigt wird. Weitere Informationen finden Sie unter „Berichte verwenden“ (S. 139).

4.9.3. Erneutes Ausführen von Aufgaben

Die Client-Installation, Deinstallation oder Update-Aufgaben können aus verschiedenen Gründen fehlschlagen. Sie müssen solche fehlgeschlagenen Aufgaben nicht neu anlegen, sondern können sie wir folgt erneut ausführen:

1. Gehen Sie zur Seite **Netzwerk > Aufgaben**.
2. Markieren Sie die Kästchen für die fehlgeschlagenen Aufgaben.

3. Klicken Sie auf die Schaltfläche **Starten** am oberen Rand der Tabelle. Die ausgewählten Aufgaben werden neu gestartet und der Aufgabenstatus wechselt auf **Neuer Versuch**.

Beachten Sie
Bei Aufgaben mit mehreren Teilaufgaben ist die Option **Starten** nur dann verfügbar, wenn alle Teilaufgaben abgeschlossen wurden. Es werden nur die fehlgeschlagenen Teilaufgaben erneut ausgeführt.

4.9.4. Aufgaben löschen

Wir empfehlen, nicht mehr benötigte Aufgaben zu löschen, um zu verhindern, dass die Aufgabenliste unübersichtlich wird.

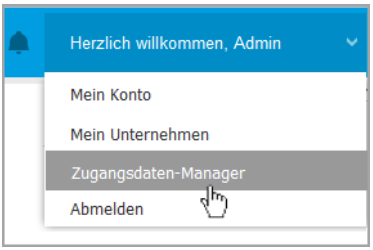
1. Gehen Sie zur Seite **Netzwerk > Aufgaben**.
2. Markieren Sie das Kästchen der Aufgabe, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen** am oberen Rand der Tabelle. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

Warnung
Wenn Sie eine ausstehende Aufgabe löschen, wird die Aufgabe auch abgebrochen. Wenn eine laufende Aufgabe gelöscht wird, werden etwaige ausstehende Teilaufgaben abgebrochen. In diesem Fall können abgeschlossene Teilaufgaben nicht rückgängig gemacht werden.

4.10. Zugangsdaten-Manager

Im Zugangsdaten-Manager können Sie die Zugangsdaten, die Sie für die Fernauthentifizierung unter den verschiedenen Betriebssystemen in Ihrem Netzwerk benötigen, definieren.

Um den Zugangsdaten-Manager zu öffnen, klicken Sie auf Ihren Benutzernamen in der rechten oberen Ecke der Seite, und wählen Sie **Zugangsdaten-Manager**.

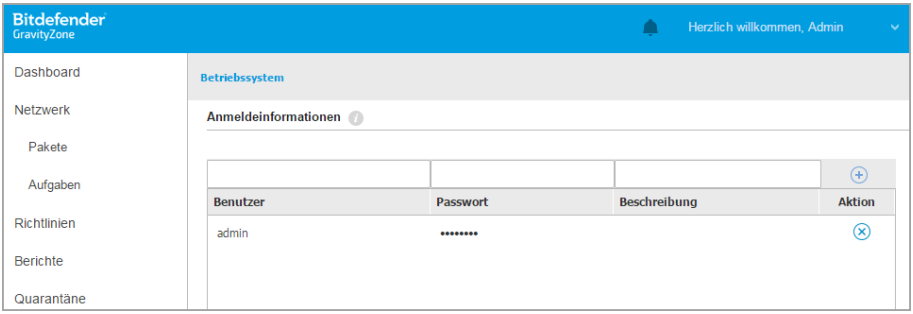


Das Zugangsdaten-Manager-Menü

4.10.1. Zugangsdaten zum Zugangsdaten-Manager hinzufügen

Mit dem Zugangsdaten-Manager können Sie die Administrator-Zugangsdaten verwalten, die für die Fernauthentifizierung während der Ausführung von Installationsaufgaben auf Computern und virtuellen Maschinen in Ihrem Netzwerk nötig sind.

So fügen Sie Zugangsdaten hinzu:



Zugangsdaten-Manager

1. Geben Sie in die entsprechenden Felder im oberen Bereich der Tabelle den Namen und das Passwort eines Administratorkontos für jedes der Betriebssysteme ein. Sie können jedem Konto eine Beschreibung hinzufügen, um es später leichter identifizieren zu können. Wenn Computer in einer Domäne sind, reicht es aus, die Anmeldeinformationen des Domänenadministrators einzugeben.

   Verwenden Sie Windows-Konventionen, wenn Sie den Namen eines Domain-Benutzerkontos eingeben, z. B. `Benutzername@domain.com` oder

`Domain\Benutzername`). Um sicherzugehen, dass die eingegebenen Zugangsdaten funktionieren, geben Sie sie in beiden Ausdrucksweisen ein (`Benutzername@domain.com` und `Domain\Benutzername`).

2. Klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** auf der rechten Seite der Tabelle. Die neuen Zugangsdaten werden der Tabelle hinzugefügt.

> **Beachten Sie**
> Wenn Sie die Authentifizierungsdaten noch nicht angegeben haben, müssen Sie diese bei Ausführung von Installationsaufgaben eingeben. Die angegebenen Zugangsdaten werden automatisch im Zugangsdaten-Manager gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben müssen.

4.10.2. Zugangsdaten aus dem Zugangsdaten-Manager löschen

So löschen Sie obsolete Zugangsdaten aus dem Zugangsdaten-Manager:

1. Bewegen Sie den Mauszeiger zur Tabellenzeile mit den Zugangsdaten, die Sie löschen möchten.
2. Klicken Sie auf die Schaltfläche ⊗ **Löschen** auf der rechten Seite der entsprechenden Tabellenzeile. Das ausgewählte Konto wird gelöscht.

5. SICHERHEITSRICHTLINIEN

Nach der Installation kann der Bitdefender-Schutz über das Control Center mit Hilfe von Sicherheitsrichtlinien konfiguriert und verwaltet werden. Eine Richtlinie legt die Sicherheitseinstellungen fest, die auf die Computer angewendet werden sollen.

Direkt nach der Installation wird den Netzwerkinventarobjekten die Standardrichtlinie zugewiesen, die mit den empfohlenen Schutzeinstellungen vorkonfiguriert ist. Die Standardrichtlinie können sie weder ändern noch löschen. Sie können Sie nur als Vorlage zur Erstellung neuer Richtlinien verwenden.

Sie können ganz nach Ihren Sicherheitsanforderungen für jede Art von verwaltetem Netzwerkobjekt beliebig viele Richtlinien erstellen.

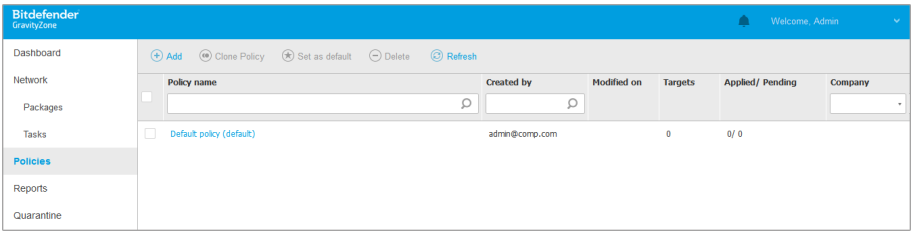
Was Sie über Richtlinien wissen sollten:

- Richtlinien werden in der **Richtlinien**übersicht erstellt und in der **Netzwerk**übersicht den Netzwerkobjekten zugewiesen.
- Netzwerkobjekte können jeweils nur eine aktive Richtlinie haben.
- Sie können eine Richtlinie einzelnen Endpunkten oder Gruppen von Endpunkten zuweisen. Standardmäßig erbt jeder Endpunkt die Richtlinie der übergeordneten Gruppe. Vererbungsoptionen können für jeden Endpunkt und für jede Gruppe von Endpunkten angepasst werden. Wenn einer Gruppe eine Richtlinie zugewiesen wird, werden die definierten Richtlinienvererbungseinstellungen berücksichtigt.
- Richtlinien werden sofort, nachdem sie angelegt oder verändert wurden, per Push an die Netzwerkobjekte übertragen. Die Einstellungen sollten in weniger als einer Minute auf den Netzwerkobjekten übernommen werden (vorausgesetzt, dass sie online sind). Wenn ein Netzwerkobjekt offline ist, werden die Einstellungen übernommen, sobald es wieder online ist.
- Die Richtlinie bezieht sich nur auf die installierten Sicherheitsmodule.
- Auf der Seite **Richtlinien** werden nur die folgenden Arten von Richtlinien angezeigt:
  - Von Ihnen erstellte Richtlinien
  - Andere Richtlinien (z. B. die Standardrichtlinie oder von anderen Benutzern erstellte Vorlagen), die Endpunkten unter Ihren Konto zugewiesen sind
- Sie können Richtlinien, die von anderen Benutzern erstellt wurden, nicht bearbeiten (es sei denn, der Ersteller der entsprechenden Richtlinie lässt dies in den Richtlinieneinstellungen zu), Sie können sie jedoch außer Kraft setzen, indem Sie den Zielobjekten eine andere Richtlinie zuweisen.

Warnung
Nur die unterstützten Richtlinienmodule werden auf den entsprechenden Endpunkten angewendet.
Bitte beachten Sie, dass für Server-Betriebssysteme nur das Malware-Schutz-Modul unterstützt wird.

5.1. Policies verwalten

Auf der **Richtlinien**-Seite können Sie die Richtlinien einsehen und verwalten.



Die Richtlinienübersicht

Bestehende Richtlinien werden in der Tabelle angezeigt. Sie können das Folgende für jede Richtlinie einsehen:

- Richtlinienname.
- Benutzer, der die Richtlinie angelegt hat.
- Datum und Zeitpunkt, zu dem die Richtlinie zuletzt verändert wurde.
- Die Anzahl der Ziele, an die die Richtlinie gesendet wurde. Klicken Sie auf die Zahl, um die entsprechenden Ziele im Netzwerkinventar anzuzeigen. Mit dieser Aktion wird ein Netzwerkinventarfilter auf der Grundlage von Richtlinienkriterien erstellt.
- Die Anzahl der Ziele, auf denen die Richtlinie angewendet wurde bzw. die Anwendung noch aussteht. Klicken Sie auf die gewünschte Zahl, um die entsprechenden Ziele im Netzwerkinventar anzuzeigen. Mit dieser Aktion wird ein Netzwerkinventarfilter auf der Grundlage von Richtlinienkriterien erstellt.

Sie können die bestehenden Richtlinien sortieren und über auswählbare Kriterien nach bestimmen Richtlinien suchen.

5.1.1. Richtlinien erstellen

Richtlinien können auf zwei Arten erstellt werden: eine neue hinzufügen oder eine bestehende kopieren (klonen).

Um eine neue Richtlinie anzulegen:

1. Gehen Sie zur **Richtlinien**-Seite.

2. Wählen Sie die Art der Richtlinienerstellung:
   - **Neue Richtlinie hinzufügen**.
     – Klicken Sie auf die Schaltfläche ⊕**Hinzufügen** am oberen Ende der Tabelle. Hierüber können Sie ausgehend von der Standardrichtlinienvorlage eine neue Richtlinie erstellen.
   - **Bestehende Richtlinie klonen**.
     a. Markieren Sie das Kästchen der Richtlinie, die Sie klonen möchten.
     b. Klicken Sie auf die Schaltfläche **Klonen** am oberen Rand der Tabelle.
3. Konfigurieren Sie die Richtlinieneinstellungen. Detaillierte Informationen finden Sie unter „Richtlinien für Computer und virtuelle Maschinen“ (S. 72).
4. Klicken Sie auf **Speichern**, um eine Richtlinie zu erstellen und zur Liste der Richtlinien zurückzukehren.

5.1.2. Richtlinieneinstellungen ändern

Richtlinieneinstellungen können zunächst beim Erstellen der Richtlinie festgelegt werden. Sie können diese später aber auch jederzeit wieder ändern.

Beachten Sie
Standardmäßig kann nur der Benutzer die Richtlinie ändern, der sie erstellt hat. Um das zu ändern, muss der Ersteller der Richtlinie auf der Seite **Details** der Richtlinie die Option **Anderen Benutzern erlauben, diese Richtlinie zu ändern** markieren.

So ändern Sie die Einstellungen einer bestehenden Richtlinie:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Finden Sie die Richtlinie in der Liste, und klicken Sie auf ihren Namen, um sie zu bearbeiten.
3. Konfigurieren Sie die Richtlinieneinstellungen nach Ihren Wünschen. Detaillierte Informationen finden Sie unter „Richtlinien für Computer und virtuelle Maschinen“ (S. 72).
4. Klicken Sie auf **Speichern**.

   Richtlinien werden sofort nach einer Änderung der Richtlinienzuweisung oder der Richtlinieneinstellungen per Push an die entsprechenden Netzwerkobjekte übertragen. Die Einstellungen sollten in weniger als einer Minute auf den Netzwerkobjekten übernommen werden (vorausgesetzt, dass sie online sind).

Wenn ein Netzwerkobjekt offline ist, werden die Einstellungen übernommen, sobald es wieder online ist.

5.1.3. Richtlinien umbenennen

Achten Sie bei Richtlinien auf einen eindeutigen Namen, damit Sie oder andere Administratoren diese schnell identifizieren können.

Um eine Richtlinie umzubenennen:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Klicken Sie auf den Richtliniennamen. Dadurch öffnet sich die Richtlinienseite.
3. Geben Sie einen neuen Namen für die Richtlinie ein.
4. Klicken Sie auf **Speichern**.

Beachten Sie
Jeder Richtlinienname ist einzigartig. Sie müssen für jede Richtlinie einen eigenen Namen eingeben.

5.1.4. Richtlinien löschen

Löschen Sie eine Richtlinie, wenn Sie sie nicht mehr länger benötigt wird. Nach dem Löschen der Richtlinie wird den Netzwerkobjekten, auf die sie zuvor angewendet wurde, die Richtlinie der übergeordneten Gruppe zugewiesen. Sollte keine andere Richtlinie angewendet werden, wird zwangsläufig die Standardrichtlinie übernommen.

Beachten Sie
Standardmäßig kann nur der Benutzer eine Richtlinie löschen, der sie erstellt hat. Um das zu ändern, muss der Ersteller der Richtlinie auf der Seite **Details** der Richtlinie die Option **Anderen Benutzern erlauben, diese Richtlinie zu ändern** markieren.

Um eine Richtlinie zu löschen:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Markieren Sie das Kästchen der Richtlinie, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche ⊖ **Löschen** am oberen Rand der Tabelle. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

5.1.5. Netzwerkobjekten Richtlinien zuweisen

Nachdem Sie die nötigen Richtlinien im Bereich **Richtlinien** eingerichtet haben, können Sie sie im Bereich **Netzwerk** bestimmten Netzwerkobjekten zuweisen.

Allen Netzwerkobjekten ist zunächst die Standardrichtlinie zugewiesen.

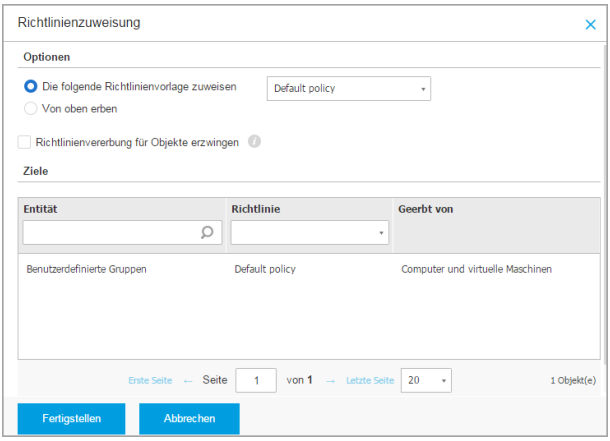
Beachten Sie
Sie können nur Richtlinien zuweisen, die auch von Ihnen erstellt wurden. Um eine Richtlinie zuzuweisen, die von einem anderen Benutzer erstellt wurde, müssen Sie sie zunächst auf der Seite **Richtlinien** klonen.

So weisen Sie eine Richtlinie zu:

1. Gehen Sie zur Seite **Netzwerk**.
2. Markieren Sie das Kästchen des gewünschten Netzwerkobjekts. Sie können ein oder mehrere Objekte auswählen, diese müssen jedoch von der selben Ebene sein.
3. Klicken Sie auf die Schaltfläche **Richtlinie zuweisen** am oberen Ende der Tabelle.

   Beachten Sie
   Sie können auch mit der rechten Maustaste auf eine Gruppe im Netzwerkbaum klicken und **Richtlinie zuweisen** aus dem Kontextmenü wählen.

   Das Fenster **Richtlinienzuweisung** wird angezeigt:



Einstellungen für die Richtlinienzuweisung

4. Konfigurieren Sie die Einstellungen für die Richtlinienzuweisung für die ausgewählten Objekte:
   - Die aktuellen Richtlinienzuweisungen für die ausgewählten Objekte können Sie in der Tabelle im Bereich **Ziele** einsehen.
   - **Die folgende Richtlinienvorlage zuweisen**. Wählen Sie diese Option aus, um den Zielobjekten eine Richtlinie aus der rechts angezeigten Liste zuzuweisen. In dieser Liste finden Sie nur die Richtlinien, die über Ihr Benutzerkonto angelegt wurden.
   - **Von oben erben**. Wählen Sie die Option **Von oben erben** aus, um den ausgewählten Netzwerkobjekten die Richtlinie der übergeordneten Gruppe zuzuweisen.
   - **Richtlinienvererbung für Objekte erzwingen**. Standardmäßig erbt jedes Netzwerkobjekt die Richtlinie der übergeordneten Gruppe. Von Änderungen der Gruppenrichtlinie sind auch alle untergeordneten Objekte dieser Gruppe davon betroffen. Dies gilt jedoch nicht für Gruppenmitglieder, denen ausdrücklich eine andere Richtlinie zugewiesen wurde.

     Wählen Sie die Option **Richtlinienvererbung für Objekte erzwingen** aus, um die ausgewählte Richtlinie auf eine Gruppe anzuwenden, und dabei auch alle untergeordneten Gruppenobjekte zu berücksichtigen, denen eine abweichende Richtlinie zugewiesen wurde. In diesem Fall zeigt die Tabelle

darunter alle untergeordneten Objekte der ausgewählten Gruppe an, die die Gruppenrichtlinie nicht erben.

5. Klicken Sie auf **Fertigstellen**, um die Änderungen zu speichern und zu übernehmen.

Richtlinien werden sofort nach einer Änderung der Richtlinienzuweisung oder der Richtlinieneinstellungen per Push an die entsprechenden Netzwerkobjekte übertragen. Die Einstellungen sollten in weniger als einer Minute auf den Netzwerkobjekten übernommen werden (vorausgesetzt, dass sie online sind). Wenn ein Netzwerkobjekt offline ist, werden die Einstellungen übernommen, sobald es wieder online ist.

Um zu überprüfen, ob die Richtlinie erfolgreich zugewiesen wurde, öffnen Sie die **Netzwerk**-Seite und klicken Sie auf den Namen des Objekts, das Sie im Fenster **Informationen** anzeigen wollen. Im Bereich **Richtlinie** können Sie den Status der aktuellen Richtlinie einsehen. Beim Status "Ausstehend" wurde die Richtlinie bisher noch nicht auf das Zielobjekt angewendet.

Den Richtlinienzuweisungsstatus können Sie auch ganz einfach im Bereich **Richtlinien** unter **Angewendet/Ausstehend** überprüfen. Klicken Sie für die gewünschte Richtlinie auf die Zahl für Zugewiesen oder Ausstehend, um auf der Seite **Netzwerk** alle Netzwerkentitäten des entsprechenden Status anzuzeigen.

5.2. Richtlinien für Computer und virtuelle Maschinen

Richtlinieneinstellungen können zunächst beim Erstellen der Richtlinie festgelegt werden. Sie können diese später aber auch jederzeit wieder ändern.

So konfigurieren Sie die Einstellungen einer Richtlinie:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Klicken Sie auf den Richtliniennamen. Dadurch öffnet sich die Richtlinieneinstellungsseite
3. Konfigurieren Sie die Richtlinieneinstellungen nach Ihren Wünschen. Es gibt die folgenden Kategorien von Einstellungen:
   - Allgemein
   - Malware-Schutz
   - Firewall
   - Inhalts -Steuer.
   - Gerätesteuerung
   - Relais

Sie können die Einstellungskategorie über das Menü auf der linken Seite auswählen.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und auf die Ziel-Computer anzuwenden. Wenn Sie die Richtlinienseite verlassen möchten, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Beachten Sie
Wie Sie Richtlinien verwenden, erfahren Sie unter „Policies verwalten“ (S. 67).

5.2.1. Allgemein

Mithilfe der allgemeinen Einstellungen können Sie für die entsprechenden Endpunkte Anzeigeoptionen, Proxy-Einstellungen, Power-User-Einstellungen, Kommunikationsoptionen und Update-Einstellungen konfigurieren.

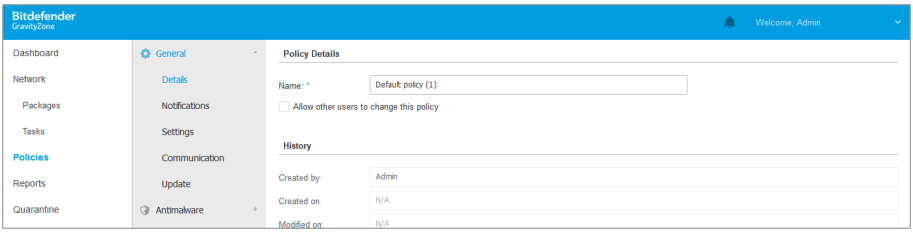
Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- Details
- Benachrichtigungen
- Einstellungen
- Kommunikation
- Update

Details

Auf der Seite Details finden Sie allgemeine Informationen zur jeweiligen Richtlinie:

- Richtlinienname
- Benutzer, der die Richtlinie angelegt hat
- Datum und Zeitpunkt, zu dem die Richtlinie erstellt wurde.
- Datum und Zeitpunkt, zu dem die Richtlinie zuletzt verändert wurde



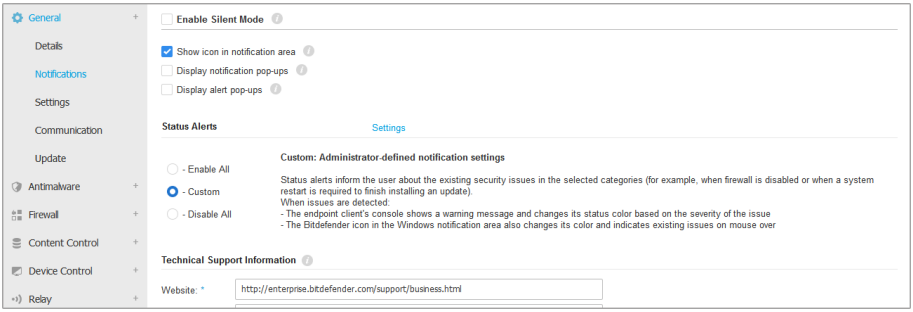
Richtlinien

Sie können die Richtlinie umbenennen, indem Sie den neuen Namen in das entsprechende Feld eingeben und unten auf der Seite auf die Schaltfläche **Speichern** klicken. Achten Sie bei Richtlinien auf einen eindeutigen Namen, damit Sie oder andere Administratoren diese schnell identifizieren können.

Beachten Sie
Standardmäßig kann nur der Benutzer die Richtlinie ändern, der sie erstellt hat. Um das zu ändern, muss der Ersteller der Richtlinie auf der Seite **Details** der Richtlinie die Option **Anderen Benutzern erlauben, diese Richtlinie zu ändern** markieren.

Benachrichtigungen

In diesem Bereich können Sie die Anzeigeoptionen für die Benutzeroberfläche des Bitdefender-Sicherheitsagenten konfigurieren.


General
Details
Notifications
Settings
Communication
Update
Antimalware
Firewall
Content Control
Device Control
Relay
Enable Silent Mode
Show icon in notification area
Display notification pop-ups
Display alert pop-ups
Status Alerts
Settings
- Enable All
- Custom
- Disable All
Custom: Administrator-defined notification settings
Status alerts inform the user about the existing security issues in the selected categories (for example, when firewall is disabled or when a system restart is required to finish installing an update).
When issues are detected:
- The endpoint client's console shows a warning message and changes its status color based on the severity of the issue
- The Bitdefender icon in the Windows notification area also changes its color and indicates existing issues on mouse over
Technical Support Information
Website: *
http://enterprise.bitdefender.com/support/business.html

Richtlinien - Anzeigeeinstellungen

- **Hintergrund-Modus aktivieren.** Über das Kästchen können Sie den Hintergrundmodus an- und ausschalten. Der Lautlos-Modus soll Ihnen helfen, Benutzereingriffe in den Sicherheitsagenten einfach zu unterbinden. Bei der

Aktivierung des Lautlos-Modus werden die folgenden Änderungen an der Richtlinienkonfiguration aktiv:

- Die Optionen **Symbol im Infobereich anzeigen**, **Benachrichtigungsfenster anzeigen** und **Warnfenster anzeigen** in diesem Bereich werden deaktiviert.
- Wenn die Firewall-Sicherheitsstufe auf **Bestehende Regeln und nachfragen** oder **Bestehende Regeln, bekannte Dateien und nachfragen** eingestellt war, wird jetzt auf **Bestehende Regeln, bekannte Dateien und zulassen** eingestellt. Ansonsten wird die Einstellung der Sicherheitsstufe nicht verändert.

- **Symbol im Infobereich anzeigen.** Wählen Sie diese Option, um das Bitdefender-Symbol im Infobereich (in der Task-Leiste) anzuzeigen. Das Symbol zeigt dem Benutzer den Sicherheitsstatus an, indem es sein Aussehen verändert und ein entsprechendes Benachrichtigungsfenster anzeigt. Außerdem kann der Benutzer mit der rechten Maustaste auf das Symbol klicken, um das Hauptfenster des Sicherheitsagenten oder das **Über**-Fenster zu öffnen. Wenn Sie das **Über**-Fenster öffnen, wird dadurch automatisch ein Bedarf-Update gestartet.
- **Benachrichtigungsfenster anzeigen.** Wählen Sie diese Option, um Benutzer mithilfe von kleinen Benachrichtigungsfenstern über wichtige Sicherheitsereignisse wie den Fund von Malware und die daraufhin ausgeführte Aktion zu informieren. Diese Benachrichtigungsfenster werden automatisch nach ein paar Sekunden ausgeblendet, ohne dass der Benutzer etwas tun muss.
- **Warnfenster anzeigen.** Anders als Benachrichtigungsfenster fordern Warnfenster Benutzer zur Auswahl einer Aktion aus. Wenn Sie Warnfenster nicht anzeigen lassen, führt Endpoint Security automatisch die empfohlene Aktion aus. Warnfenster werden in den folgenden Situationen angezeigt:
  - Wenn die Firewall so konfiguriert ist, dass der Benutzer entscheidet, welche Aktion ausgeführt wird, wenn unbekannte Anwendungen auf Netzwerk oder Internet zugreifen wollen.
  - Wenn Active Virus Control/Angriffserkennungssystem aktiviert wird, wenn eine potenziell schädliche Anwendung gefunden wird.
  - Wenn der Geräte-Scan aktiviert ist und ein externes Speichermedium an den Computer angeschlossen wird. Diese Einstellung kann unter **Malware-Schutz > Bei Bedarf** vorgenommen werden.
- **Statusbenachrichtigungen.** Benutzer werden auf Konfigurationsprobleme in der Sicherheit ihres Endpunktes durch Statusbenachrichtigungen hingewiesen.

So werden Benutzer zum Beispiel darauf hingewiesen, wenn ein Problem im Malware-Schutz besteht, zum Beispiel wenn das Zugriff-Scan-Modul deaktiviert ist oder ein vollständiger Systemscan überfällig ist.

Benutzer werden über Ihren Schutzstatus auf zwei Wegen informiert:

- im Infobereich des Hauptfensters, der eine entsprechende Statusnachricht anzeigt und seine Farbe je nach der Schwere der Sicherheitsprobleme ändert. Über einen Klick auf die entsprechende Schaltfläche können Benutzer Details zum jeweiligen Problem anzeigen.
- durch das Bitdefender-Symbol in der Task-Leiste, das sich ändert, wenn Probleme entdeckt werden.

Der Bitdefender-Sicherheitsagent verwendet die folgende Farbcodierung im Infobereich:

- Grün: keine Probleme gefunden.
- Gelb: Auf dem Endpunkt gibt es nicht-kritische Probleme mit der Sicherheit. Benutzer müssen ihre Arbeit nicht unbedingt unterbrechen, um diese Probleme zu beheben.
- Rot: Auf dem Endpunkt gibt es kritische Probleme, die umgehende Aufmerksamkeit erfordern.

Sie können den Benachrichtigungen an Ihre Bedürfnisse anpassen. Wählen Sie eine der folgenden Stufen: (**Alle aktivieren**, **Benutzerdefiniert**, **Alle deaktivieren**). Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.

So passen Sie die Benachrichtigungen im Detail an:

1. Wählen Sie die Stufe **Benutzerdefiniert**.
2. Klicken Sie auf den Link **Einstellungen**, um das Konfigurationsfenster zu öffnen.
3. Wählen Sie die Sicherheitsaspekte aus, die überwacht werden sollen. Für jede Kategorie können Sie einstellen, ob die Benachrichtigung als Warnung, als kritisches Problem oder gar nicht angezeigt werden soll. Sie haben diese Optionen:
   - **Allgemein**. Eine Statusbenachrichtigung wird ausgegeben, wenn ein Systemneustart während oder nach eines Produktwartungsvorgangs

erforderlich wird und auch wenn der Sicherheitsagent keine Verbindung zu Bitdefender Cloud Services herstellen konnte.

- **Malware-Schutz**. In den folgenden Situationen werden Statusbenachrichtigungen ausgegeben:
  - Zugriff-Scans sind aktiviert, aber viele lokale Dateien werden übersprungen.
  - Seit dem letzten vollständigen Systemscan auf der Maschine ist eine bestimmte Anzahl an Tagen verstrichen.

    Sie können festlegen, wie die Benachrichtigungen angezeigt werden und wie viele Tage der letzte vollständige Systemscan her sein darf.
  - Zum Abschluss eines Desinfektionsvorgangs muss ein Neustart durchgeführt werden.
- **Firewall**. Diese Statusbenachrichtigung wird ausgegeben, wenn das Firewall-Modul deaktiviert ist.
- **Inhaltssteuerung**. Diese Statusbenachrichtigung wird ausgegeben, wenn das Inhaltssteuerungsmodul deaktiviert ist.
- **Update**. Die Statusbenachrichtigung wird immer dann ausgegeben, wenn ein Systemneustart durchgeführt werden muss, um einen Update-Vorgang abzuschließen.

- **Informationen zum technischen Support.** Durch Ausfüllen der entsprechenden Felder können Sie die im **Über**-Fenster des Sicherheitsagenten angezeigten Informationen zum technischen Support und Kontaktdaten selbst anpassen. Benutzer können auf diese Informationen aus der Konsole des Sicherheitsagenten zugreifen, indem sie mit der rechten Maustaste auf das Bitdefender-Symbol in der Task-Leiste klicken und anschließend **Über** wählen.

Einstellungen

In diesem Bereich können Sie die folgenden Einstellungen konfigurieren:

- **Passwortkonfiguration.** Um zu verhindern, dass Benutzer mit Administratorenrechten den Schutz deinstallieren, müssen Sie ein Passwort festlegen.

  Das Deinstallationspasswort kann schon vor der Installation festgelegt werden, indem Sie das Installationspaket individuell anpassen. Falls Sie dies getan

haben, wählen Sie **Installationseinstellungen beibehalten**, um das aktuelle Passwort beizubehalten.

Um das Passwort einzurichten oder das aktuelle Passwort zu ändern, wählen Sie **Passwort aktivieren** und geben Sie das gewünschte Passwort ein. Um den Passwortschutz zu entfernen, wählen Sie **Passwort deaktivieren**.

- **Proxy-Konfiguration**

  Wenn sich Ihr Netzwerk hinter einem Proxy-Server befindet, müssen Sie die Proxy-Einstellungen angeben, mithilfe derer Ihre Endpunkte mit den GravityZone-Komponenten kommunizieren können. In diesem Fall müssen Sie die Option **Proxy-Konfiguration** aktivieren und die entsprechenden Parameter eingeben:
  - **Server** - Geben Sie die IP-Adresse des Proxy-Servers ein
  - **Port** - Geben Sie den Port ein, über den die Verbindung zum Proxy-Server hergestellt wird.
  - **Benutzername** - Geben Sie einen für den Proxy-Server gültigen Benutzernamen ein.
  - **Passwort** – Geben Sie hier das gültige Passwort für den entsprechenden Benutzer ein.

- **Power -User**

  Mit dem Power-User-Modul können Benutzern auf Endpunkt-Ebene Administratorrechte verliehen werden, mit denen diese Benutzer über Bitdefender Endpoint Security Tools Richtlinieneinstellungen anzeigen und verändern können.

  Wenn Sie für bestimmte Endpunkte Power-User-Rechte festlegen möchten, müssen Sie dieses Modul zunächst in den Sicherheitsagenten, der auf den entsprechenden Endpunkten installiert ist, integrieren. Danach müssen Sie die Power-User-Einstellungen in der diesen Endpunkten zugewiesenen Richtlinie konfigurieren:

  Wichtig
  Das Power-User-Modul besteht nur für unterstützte Windows-Desktop- und -Server-Betriebssysteme zur Verfügung.

  1. Aktivieren Sie die Option **Power-User**.
  2. Legen Sie in den Feldern darunter ein Power-User-Passwort fest.

Benutzer, die von einem lokalen Endpunkt aus in den Power-User-Modus wechseln möchten, werden dann aufgefordert, dieses Passwort einzugeben.

Benutzer können das Power-User-Modul öffnen, indem sie mit der rechten Maustaste auf das Bitdefender-Symbol in ihrer Task-Leiste klicken und dann aus dem Kontextmenü **Power-User** de wählen. Nach Eingabe des Passworts im Anmeldefenster wird eine Konsole geöffnet, in der der Benutzer die Richtlinieneinstellungen sehen und ändern kann.

Beachten Sie
Über die Power-User-Konsole kann lokal nur auf bestimmte Sicherheitsfunktionen zugegriffen werden: Malware-Schutz, Firewall, Inhaltssteuerung und Gerätesteuerung.

So können Sie die Änderungen rückgängig machen, die im Power-User-Modus gemacht wurden:

- Öffnen Sie im Control Center die Richtlinienvorlage, die dem Endpunkt mit Power-User-Rechten zugewiesen ist, und klicken Sie auf **Speichern**. So werden die ursprünglichen Einstellungen wieder auf den Endpunkt angewendet.
- Weisen Sie dem Endpunkt mit Power-User-Rechten eine neue Richtlinie zu.
- Melden Sie sich lokal an dem Endpunkt an, öffnen Sie die Power-User-Konsole und klicken Sie auf **Erneut synchronisieren**.

So finden Sie schnell Endpunkte, deren Richtlinien im Power-User-Modus verändert wurden:

- Klicken Sie auf der Seite **Netzwerk** auf das Menü **Filter** und markieren Sie dann im Reiter **Richtlinie** das Kästchen **Bearbeitet vom Power-User**.
- Klicken Sie auf der Seite **Netzwerk** auf den gewünschten Endpunkt um das Fenster **Informationen** zu öffnen. Wenn die Richtlinie im Power-User-Modus verändert wurde, wird im Bereich **Richtlinie** des Reiters **Allgemein** ein Hinweis angezeigt.

Wichtig
Das Power-User-Modul dient in erster Linie zur Fehlerbehebung, denn mit diesem Modul kann der Netzwerkadministrator unkompliziert Richtlinieneinstellungen auf lokalen Computern anzeigen und ändern. Die Vergabe von Power-User-Rechten innerhalb des Unternehmens muss auf befugte Personen beschränkt bleiben, um

sicherzustellen, dass die Sicherheitsrichtlinien stets auf alle Endpunkte im Unternehmensnetzwerk angewendet werden.

- **Optionen**

  In diesem Bereich können Sie die folgenden Einstellungen festlegen:

  - **Ereignisse entfernen, die älter sind als (Tage).** Bitdefender security agent führt ein detailliertes Ereignisprotokoll über alle Aktivitäten der Software auf Ihrem Computer (einschließlich der Computer-Aktivitäten, die von der Inhaltssteuerung überwacht werden). Ereignisse werden standardmäßig nach 30 Tagen aus dem Protokoll gelöscht. Um dieses Intervall zu ändern, wählen Sie im Menü eine andere Option aus.
  - **Berichte über Systemabstürze an Bitdefender schicken.** Wählen Sie diese Option, damit Berichte zur Analyse an die Bitdefender-Labors geschickt werden, wenn der Sicherheitsagent abstürzt. Die Berichte helfen unseren Mitarbeitern dabei, die Ursache des Problems zu finden und ein Wiederauftreten zu verhindern. Es werden keine persönlichen Informationen mitgesendet.

Kommunikation

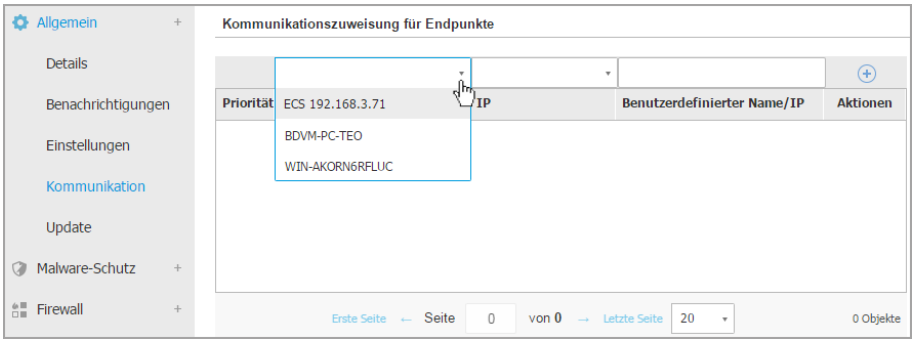
In diesem Bereich können Sie den gewünschten Endpunkten eine oder mehrere Relais-Maschinen zuweisen und dann die Proxy-Einstellungen für die Kommunikation zwischen diesen Endpunkten und der GravityZone konfigurieren.

Kommunikationszuweisung für Endpunkte

Wenn im Zielnetzwerk mehrere Relais-Agenten verfügbar sind, können Sie den ausgewählten Computern per Richtlinie einen oder mehrere Relais-Endpunkte zuweisen.

So weisen Sie Ziel-Computern Relais-Endpunkte zu:

1. Klicken Sie in der Tabelle **Kommunikationszuweisung für Endpunkte** auf das Feld **Name**. Die Liste der in Ihrem Netzwerk erkannten Relais-Endpunkte wird angezeigt.
2. Wählen Sie eine Entität.



Richtlinien - Kommunikationseinstellungen

3. Klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** auf der rechten Seite der Tabelle.

   Der Relais-Endpunkt wird der Liste hinzugefügt. Alle Zielcomputer werden über die angegebenen Relais-Endpunkt mit dem Control Center kommunizieren.

4. Wiederholen Sie diese Schritte, wenn Sie mehrere Relais (sofern vorhanden) hinzufügen möchten.

5. Sie können die Priorität der Relais-Endpunkte konfigurieren, indem Sie auf die rechts von jeder Entität angezeigten Pfeile ⌃ hoch und ⌄ rnter klicken. Die Kommunikation mit den Zielcomputern läuft über die Entität, die ganz oben in der Liste steht. Sollte die Kommunikation über diese Entität nicht möglich sein, wird es über die nächste in der Liste versucht.

6. Um eine Entität aus der Liste zu entfernen, klicken Sie auf die entsprechende Schaltfläche ⊗ **Löschen** auf der rechten Seite der Tabelle.

Kommunikation zwischen Endpunkte und Relais / GravityZone

In diesem Bereich können Sie die Proxy-Einstellungen für die Kommunikation zwischen den Zielendpunkten und den zugewiesenen Relais-Maschinen, bzw. für den Fall, dass kein Relais zugewiesen wurde, zwischen den Zielendpunkten und dem GravityZone Control Center konfigurieren.

- **Installationseinstellungen behalten**, wenn dieselben Proxy-Einstellungen verwendet werden sollen, die im Installationspaket definiert sind.

- **Den im Bereich Allgemein definierten Proxy verwenden**, wenn Sie die Proxy-Einstellungen verwenden möchten, die in der aktuellen Richtlinie im Bereich **Allgemein > Einstellungen** definiert sind.
- **Nicht verwenden**, wenn die Zielendpunkte nicht über einen Proxy mit den GravityZone-Komponenten kommunizieren.

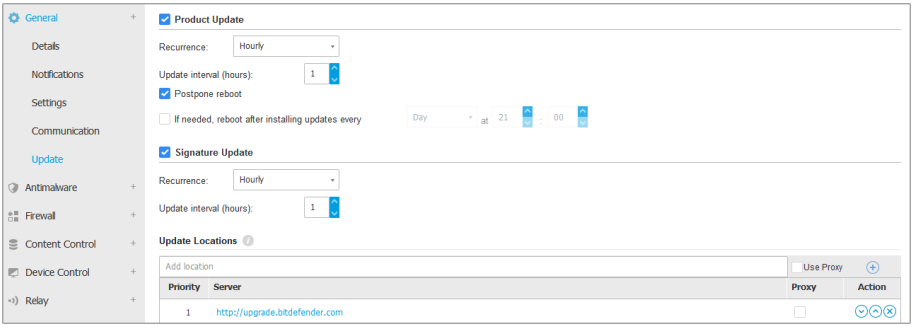
Kommunikation zwischen Endpunkte und Cloud Services

In diesem Bereich können Sie die Proxy-Einstellungen für die Kommunikation zwischen den Zielendpunkten und Bitdefender Cloud Services konfigurieren:

- **Installationseinstellungen behalten**, wenn dieselben Proxy-Einstellungen verwendet werden sollen, die im Installationspaket definiert sind.
- **Den im Bereich Allgemein definierten Proxy verwenden**, wenn Sie die Proxy-Einstellungen verwenden möchten, die in der aktuellen Richtlinie im Bereich **Allgemein > Einstellungen** definiert sind.
- **Nicht verwenden**, wenn die Zielendpunkte nicht über einen Proxy mit den GravityZone-Komponenten kommunizieren.

Update

In diesem Bereich können Sie die Update-Einstellungen für Bitdefender-Sicherheitsagenten und Virensignaturen konfigurieren. Updates sind von großer Wichtigkeit, da nur so den neuesten Bedrohungen begegnet werden kann.



Richtlinien - Update-Optionen

- **Produkt-Update.** Der Bitdefender-Sicherheitsagent wird stündlich automatisch nach Updates suchen und diese herunterladen und installieren (Standardeinstellung). Automatische Updates werden unauffällig im Hintergrund durchgeführt.
  - **Wiederholung**. Um die automatische Update-Wiederholung zu ändern, wählen Sie eine andere Option von der Menüleiste und konfigurieren Sie es nach Ihren Bedürfnissen, in den folgenden Feldern.
  - **Neustart aufschieben**. Manche Updates machen einen Neustart des Systems erforderlich, um die Installation abzuschließen. Wenn Sie diese Option auswählen, wird das Programm weiterhin mit den alten Dateien arbeiten, bis der Computer neu gestartet wird, ohne den Nutzer vorher zu informieren. Ansonsten wird eine Benachrichtigung in der Benutzeroberfläche den Benutzer auffordern, das System neu starten, sollte dies wegen eines Updates erforderlich sein.
  - Wenn Sie den Zeitpunkt des Neustarts verschieben möchten, können Sie eine passendere Zeit festlegen, zu der die Computer automatisch neu gestartet werden, sollte dies (weiterhin) nötig sein. Dies erweist sich insbesondere bei Servern als sehr nützlich. Klicken Sie auf **Wenn nötig, nach der Installation von Updates neu starten** und legen Sie eine passende Zeit für den Neustart fest (täglich, wöchentlich an einem bestimmten Tag, zu einer bestimmten Uhrzeit).
- **Virensignatur-Update.** Der Bitdefender-Sicherheitsagent wird stündlich automatisch nach Signatur-Updates suchen (Standardeinstellung). Automatische Updates werden unauffällig im Hintergrund durchgeführt. Um die automatische Update-Wiederholung zu ändern, wählen Sie eine andere Option von der Menüleiste und konfigurieren Sie es nach Ihren Bedürfnissen, in den folgenden Feldern.
- **Update-Adressen**. Der Standard-Update-Server für Bitdefender-Sicherheitsagenten ist http://upgrade.bitdefender.com. Sie können einen anderen Update-Server festlegen, indem Sie die IP-Adresse oder den lokalen Hostnamen einer oder mehrerer Relais-Maschinen in Ihrem Netzwerk eingeben und dann deren Priorität mithilfe der Pfeile festlegen, die angezeigt werden, wenn Sie mit dem Mauszeiger auf den jeweiligen Server gehen. Wenn der erste Update-Server in der Liste nicht verfügbar ist, wird der zweite verwendet usw.

  Um die lokale Update-Adresse einzurichten:

1. Geben Sie die Adresse des lokalen Update-Servers in das Feld **Ziel hinzufügen** ein. Verwenden Sie dazu eine der folgenden Syntaxoptionen:
   - `update_server_ip:port`
   - `update_server_name:port`

   Der Standard-Port ist 7074.
2. Falls sich Client-Computer über einen Proxy-Server mit dem lokalen Update-Server verbinden, aktivieren Sie **Proxy benutzen**.
3. Klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** auf der rechten Seite der Tabelle.
4. Legen Sie mithilfe der Pfeile ⌃ und ⌄ in der Spalte **Aktion** die Priorität der definierten Udpate-Server fest. Wenn der erste Update-Server in der Liste nicht verfügbar ist, wird der zweite verwendet usw.

Um einen Pfad aus der Liste zu löschen, klicken Sie auf die entsprechende ⊗ **Löschen**-Schaltfläche. Es ist zwar möglich, die standardmäßige Update-Adresse zu entfernen, dies wird jedoch nicht empfohlen.

5.2.2. Malware-Schutz

Das Modul für den Malware-Schutz schützt Sie vor allen Arten von Bedrohungen durch Malware (Viren, Trojaner, Spyware, Rootkits, Adware usw.). Der Schutz wird in zwei Kategorien unterteilt:

- Zugriff-Scans: Verhindern, dass neue Malware-Bedrohungen auf das System gelangen.
- Bedarf-Scans: Malware, die sich bereits im System befindet, kann entdeckt und entfernt werden.

Wenn der Bitdefender-Sicherheitsagent einen Virus oder andere Malware findet, versucht das Programm automatisch, den Malware-Code aus der infizierten Datei zu entfernen und die Originaldatei wiederherzustellen. Diese Operation bezeichnet man als Desinfektion. Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infektion zu isolieren. In der Quarantäne kann ein Virus keinen Schaden anrichten, denn er kann weder ausgeführt noch geöffnet werden.

Erfahrene Benutzer können Scan-Ausschlüsse konfigurieren, wenn Sie nicht möchten, dass bestimmte Dateien oder Dateitypen gescannt werden.

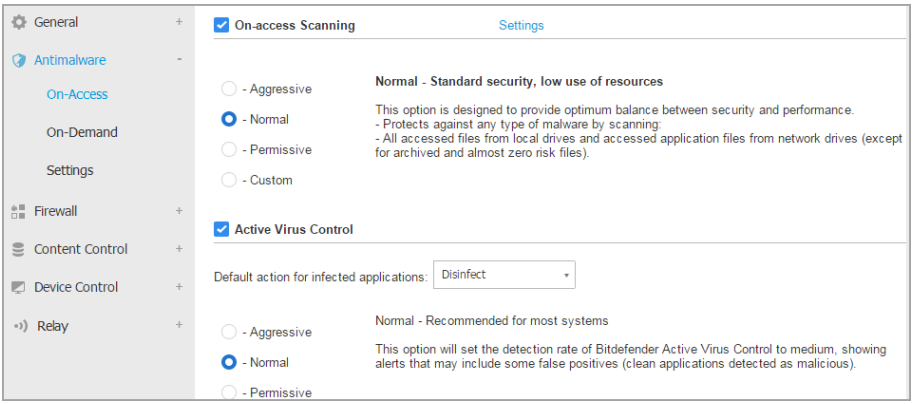
Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- Zugriff
- Bedarf-Scan
- Einstellungen

Zugriff

In diesem Anschnitt können Sie die zwei Komponenten für den Echtzeit-Malware-Schutz konfigurieren:

- Zugriff-Scan
- Active Virus Control


General
Antimalware
On-Access
On-Demand
Settings
Firewall
Content Control
Device Control
Relay
On-access Scanning
Settings
- Aggressive
- Normal
- Permissive
- Custom
Normal - Standard security, low use of resources
This option is designed to provide optimum balance between security and performance.
- Protects against any type of malware by scanning:
- All accessed files from local drives and accessed application files from network drives (except for archived and almost zero risk files).
Active Virus Control
Default action for infected applications:
Disinfect
- Aggressive
- Normal
- Permissive
Normal - Recommended for most systems
This option will set the detection rate of Bitdefender Active Virus Control to medium, showing alerts that may include some false positives (clean applications detected as malicious).

Richtlinien - Zugriff-Scan-Einstellungen

Zugriff-Scan

Zugriff-Scans verhindern, dass neue Malware auf das System gelangt, indem lokale und Netzwerk-Dateien gescannt werden, sobald auf sie zugegriffen wird (öffnen, verschieben, kopieren oder ausführen). Ferner werden Boot-Sektoren und potenziell unerwünschte Anwendungen (PUA) gescannt.

Um die Zugriffs-Scans zu konfigurieren:

1. Über das Kästchen können Sie Zugriffs-Scans aktivieren oder deaktivieren.

Warnung
Wenn Sie Zugriff-Scans deaktivieren, werden die Endpunkte anfällig für Malware.

2. Für eine schnelle Konfiguration, klicken Sie auf die Sicherheitsstufe, die Ihren Anforderungen entspricht (aggressiv, normal, tolerant). Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.
3. Sie können Details der Scan-Einstellungen konfigurieren, indem Sie die Sicherheitsstufe **Benutzerdefiniert** wählen und auf den Link **Einstellungen** klicken. Das Fenster für die **Zugriff-Scan-Einstellungen** wird angezeigt. Hier finden Sie unter den Reitern **Allgemein** und **Erweitert** eine Reihe von Optionen. Im Folgenden werden die Optionen vom ersten bis zum letzten Reiter beschrieben:
   - **Datei-Speicherort**. Verwenden Sie diese Optionen, um festzulegen, welche Dateien gescannt werden sollen. Die Scan-Einstellungen für lokale Dateien (auf dem lokalen Endpoint gespeichert) und Netzwerkdateien (auf den Netzwerklaufwerken gespeichert) können separat festgelegt werden. Wenn der Malware-Schutz auf allen Computern im Netzwerk installiert ist, ist es möglich, den Scan der Netzwerkdateien zu deaktivieren, um den Netzwerkzugriff zu beschleunigen.

     Sie können den Sicherheitsagenten so einrichten, dass Scans entweder für alle aufgerufenen Dateien (unabhängig von der Dateiendung), oder nur für Anwendungsdateien oder nur für bestimmte Dateiendungen, die Sie für gefährlich erachten, durchgeführt werden. Das Scannen aller Dateien bietet den besten Schutz, während das ausschließliche Scannen der Anwendungen nur für die Verbesserung der Systemleistung verwendet werden kann.

     Beachten Sie
     Anwendungsdateien sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen. Weitere Informationen finden Sie unter „Anwendungsdateitypen“ (S. 176).

     Wenn Sie nur bestimmte Dateiendungen scannen lassen möchten, wählen Sie **Benutzerdefinierte Endungen** aus dem Menü, und geben Sie dann die Endungen in das Eingabefeld ein. Klicken Sie nach jeder Eingabe auf `Speichern`.

     Sie können auch große Dateien vom Scan ausschließen, um die Systemleistung nicht zu stark zu beeinträchtigen. Markieren Sie das Kästchen **Maximale Größe (MB)** geben Sie die Größe an, bis zu der Dateien gescannt werden sollen. Gehen Sie mit dieser Einstellung vorsichtig um, denn Malware kann auch größere Dateien befallen.

- **Scan.** Markieren Sie die entsprechenden Kästchen, um die gewünschten Scan-Optionen zu aktivieren.
  - **Nur neue oder geänderte Dateien.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
  - **Boot-Sektoren.** Prüft die Bootsektoren des Systems. Dieser Sektor der Festplatte beinhaltet den notwendigen Code um den Boot-Prozess zu starten. Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.
  - **Für Keylogger.** Keylogger zeichnen auf, was Sie auf Ihrer Tastatur tippen, und schicken dann via Internet Berichte an Hacker. Der Hacker kann über diese gestohlenen Daten sensible Informationen erfahren, so wie Kontonummern und Passwörter und kann Sie zu seinem eigenen Profit verwenden.
  - **Für potenziell unerwünschte Anwendungen (PUA).** Eine potenziell unerwünschte Anwendung (PUA) ist ein Programm, das auf dem PC vermutlich nicht erwünscht ist und häufig in Verbindung mit Freeware installiert wurde. Diese Art von Programmen kann ohne Zustimmung des Benutzers installiert werden (wird auch als Adware bezeichnet) oder wird standardmäßig bei der Express-Installation mitinstalliert (werbeunterstützt). Diese Programme können Pop-up-Werbung anzeigen, unerwünschte Symbolleisten im Standard-Browser installieren oder Hintergrundprozesse ausführen und so den PC verlangsamen.
  - **Archive**. Wählen Sie diese Option, wenn Sie Zugriff-Scans für archivierte Dateien aktivieren möchten. Das Scannen von Archiven ist ein langsamer und ressourcen-intensiver Vorgang, der aus diesem Grund nicht für den Echtzeitschutz empfohlen wird. Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für die Systemsicherheit. Die Malware kann das System nur beeinträchtigen, wenn die infizierte Datei aus dem Archiv extrahiert und bei deaktivierten Zugriff-Scans ausgeführt wird.

    Sollten Sie sich zur Verwendung dieser Option entscheiden, können Sie die folgenden Optimierungsoptionen konfigurieren:
    - **Maximale Archivgröße (MB).** Sie können Sie die maximale Größe der Archive angeben, die beim Zugriff-Scan durchsucht werden sollen. Markieren Sie das entsprechende Kästchen und geben Sie die maximale Archivgröße in MB ein.

- **Maximale Archivtiefe (Ebenen).** Markieren Sie das entsprechende Kästchen und wählen Sie die maximale Archivtiefe aus dem Menü. Für optimale Leistung wählen Sie den niedrigsten Wert, für maximalen Schutz wählen Sie den höchsten Wert.

- **Prüfaktionen**. Abhängig vom gefundenen Dateityp werden folgende Aktionen automatisch ausgeführt:
  - **Standardaktion für infizierte Dateien.** Als infiziert eingestufte Dateien stimmen mit einer Malware-Signatur der Bitdefender Malware-Signaturen-Datenbank überein. Der Bitdefender-Sicherheitsagent kann normalerweise den Malware-Code aus einer infizierten Datei entfernen und die ursprüngliche Datei rekonstruieren. Diesen Vorgang bezeichnet man als Desinfektion.

    Wenn eine infizierte Datei gefunden wird, versucht der Bitdefender-Sicherheitsagent automatisch, diese zu desinfizieren. Falls die Desinfizierung fehlschlägt, wird die Datei in die Quarantäne verschoben, um dort die Infizierung einzudämmen.

    Wichtig
    Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

  - **Standardaktion für verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert. Da es sich bei B-HAVE um eine heuristische Analysetechnologie handelt, kann Bitdefender-Sicherheitsagent nicht sicher sein, ob die Datei tatsächlich mit Malware infiziert ist. Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.

    Wenn eine verdächtige Datei gefunden wird, wird den Benutzern der Zugriff auf diese Datei verwehrt, um eine potenzielle Infektion zu verhindern.

  Sie können die standardmäßigen Aktionen verändern, dies wird aber nicht empfohlen. Sie können für jeden Dateityp zwei Aktionen festlegen. Folgende Aktionen stehen zur Verfügung:

  Zugriff verweigern
  Zugriff auf infizierte Dateien verweigern.

Wichtig
Bei Mac-Endpunkten wird statt der Aktion **Zugriff verweigern** die Aktion **In die Quarantäne verschieben** ausgeführt.

Desinfizieren
Den Malware-Kode aus den entdeckten infizierten Dateien entfernen. Es wird empfohlen, dass dies immer die erste Aktion bleibt, die für infizierte Dateien durchgeführt wird.

Löschen
Infizierte Dateien ohne vorherige Benachrichtigung von der Festplatte löschen. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.

Dateien in Quarantäne verschieben
Verschieben Sie infizierte Dateien von ihrem Speicherort in den Quarantäne-Ordner. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. Sie können die Dateien in Quarantäne über die Quarantäne-Seite in der Konsole verwalten.

Active Virus Control

Active Virus Control von Bitdefender ist eine innovative und vorbeugende Erkennungstechnologie, die hoch entwickelte heuristische Methoden nutzt, um mögliche neue Bedrohungen in Echtzeit zu erkennen.

Active Virus Control überwacht kontinuierlich die auf Ihrem Endpunkt laufenden Anwendungen auf Malware-ähnliche Aktionen. Jede dieser Aktionen wird eingestuft, für jeden Prozess wird weiterhin eine Allgemeineinstufung erstellt. Wenn diese Gesamteinstufung einen bestimmten Grenzwert überschreitet, wird der entsprechende Prozess als schädlich eingestuft. Active Virus Control wird automatisch versuchen, die gefundene Datei zu desinfizieren. Wenn die Desinfektionsroutine fehlschlägt, löscht Active Virus Control die Datei. Weitere Informationen erhalten Sie im Active-Virus-Control-Whitepaper auf unserer Website.

Beachten Sie
Bevor die Desinfektion durchgeführt wird, wird eine Kopie der Datei in der Quarantäne abgelegt, damit Sie die Datei bei Bedarf später wiederherstellen können. Diese Aktion kann im Reiter **Malware-Schutz > Einstellungen** der Richtlinieneinstellungen mit der Option **Dateien vor der Desinfektion in die Quarantäne kopieren** konfiguriert werden. Diese Option ist in den Richtlinienvorlagen standardmäßig aktiviert.

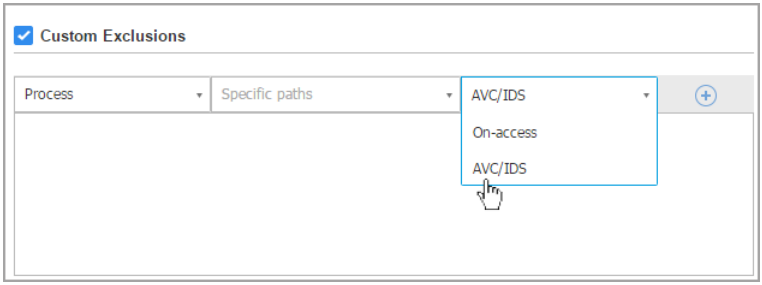
Konfiguration der Active Virus Control:

1. Über das Kästchen können Sie Active Virus Control aktivieren oder deaktivieren.

   Warnung
   Wenn Sie Active Virus Control deaktivieren, werden die Computer anfällig für unbekannte Malware.

2. Die Standardaktion für infizierte Anwendungen, die von Active Virus Control gefunden werden, ist Desinfektion. Über das Menü kann eine andere Standardaktion gewählt werden.
3. Klicken Sie auf die Sicherheitsstufe, die Ihren Ansprüchen entspricht (aggressiv, normal oder tolerant). Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.

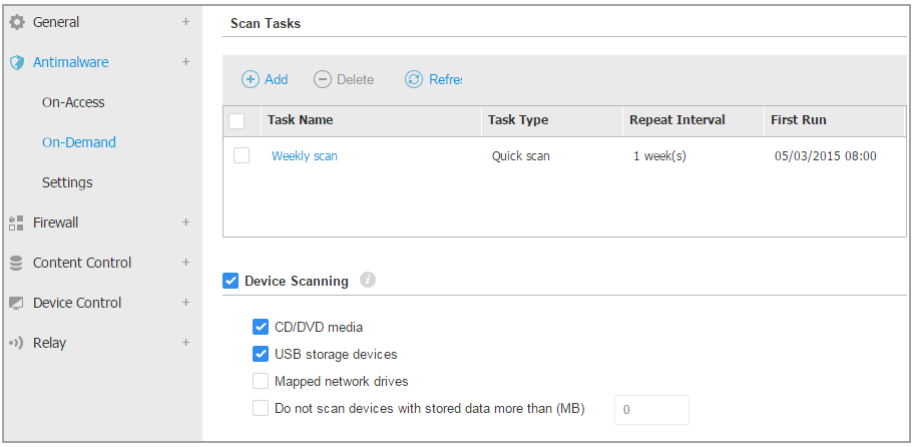
   Beachten Sie
   Je höher Sie die Sicherheitsstufe einstellen, desto weniger Anzeichen verdächtiger Aktivitäten braucht Active Virus Control, um einen Prozess zu melden. Dadurch steigt die Zahl der gemeldeten Anwendungen, aber auch die Wahrscheinlichkeit von Fehlalarmen (ungefährlichen Anwendungen, die dennoch als schädlich eingestuft wurden).
   Es wird dringend empfohlen, Ausschlussregeln für häufig genutzte oder bekannte Anwendungen zu erstellen, um Fehlalarme zu vermeiden (ungefährliche Anwendungen, die fälschlicherweise erkannt werden). Klicken Sie auf den Reiter Malware-Schutz > Einstellungen und konfigurieren Sie die AVC/IDS-Prozessausschlussregeln für vertrauenswürdige Anwendungen.



Richtlinien - AVC/IDS-Prozessauschluss

Bedarf-Scan

In diesem Bereich können Sie Malware-Scan-Aufgaben hinzufügen und konfigurieren, die dann regelmäßig nach einem festgelegten Zeitplan auf den Ziel-Computern ausgeführt werden.



Richtlinien - Bedarf-Scan-Aufgaben

Das Scannen wird im Hintergrund durchgeführt. Der Benutzer wird darüber informiert, dass der Scan-Prozess nur über ein Symbol ausgeführt werden kann, das in dem Benachrichtigungsfeld erscheint.

Obwohl nicht zwingend erforderlich, empfiehlt es sich, einen umfassenden System-Scan einzuplanen, der wöchentlich auf allen Endpunkten ausgeführt wird. Regelmäßige Scans der Endpunkte bieten vorbeugende Sicherheit. Nur so können Malware-Bedrohungen erkannt und blockiert werden, die den Echtzeitschutz unter Umständen umgangen haben.

Neben den regelmäßigen Scans können Sie auch eine automatische Erkennung und Prüfung von externen Speichermedien konfigurieren.

Scan-Aufgaben verwalten

Die Scan-Aufgaben-Tabelle informiert Sie über bestehende Scan-Aufgaben und enthält wichtige Informationen zu den einzelnen Aufgaben:

- Name und Art der Aufgabe.

- Zeitplan, anhand dessen die Aufgabe regelmäßig ausgeführt wird (Wiederholung).
- Zeitpunkt, zu dem die Aufgabe das erste Mal ausgeführt wurde.

Sie können die folgenden Typen von Scan-Aufgaben hinzufügen und konfigurieren:

- **Quick Scan** setzt auf In-the-Cloud-Scans, um auf Ihrem System laufende Malware aufzuspüren. Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenscan in Anspruch nehmen würde.

  Der Quick-Scan ist eine Standard-Scan-Aufgabe mit vorkonfigurierten Optionen, die nicht geändert werden können. Pro Richtlinie können Sie nur eine Quick-Scan-Aufgabe hinzufügen.

- Der **Vollständige Scan** durchsucht den gesamten Endpunkt nach allen Typen von Malware, die ein Sicherheitsrisiko darstellen, z. B. Viren, Spyware, Adware, Rootkits usw.

  Der Vollständige Scan ist eine Standard-Scan-Aufgabe mit vorkonfigurierten Optionen, die nicht geändert werden können. Pro Richtlinie können Sie nur eine Vollständiger-Scan-Aufgabe hinzufügen.

- Bei einem **benutzerdefinierten Scan** können Sie die Orte, die gescannt werden sollen, selbst auswählen und die Scan-Optionen festlegen.

- **Netzwerk-Scan** ist ein benutzerdefinierten Scan, bei dem Sie zunächst einen einzelnen verwalteten Endpunkt bestimmen, über den Netzwerklaufwerke gescannt werden, und dann die Scan-Optionen und die zu scannenden Speicherorte konfigurieren können. Für Netzwerk-Scan-Aufgaben müssen Sie die Zugangsdaten eines Benutzerkontos mit Lese- und Schreibberechtigung auf den entsprechenden Netzwerklaufwerken eingeben, damit der Sicherheitsagent auf diese Netzwerklaufwerke zugreifen und die entsprechenden Aktionen durchführen kann.

  Die wiederkehrende Netzwerk-Scan-Aufgabe wird nur an den ausgewählten Scanner-Endpunkt gesendet. Wenn der entsprechende Endpunkt nicht verfügbar ist, werden die Einstellungen für lokalen Scan angewendet.

  Beachten Sie
  Netzwerk-Scan-Aufgaben können Sie nur innerhalb einer Richtlinie erstellen, die bereits einem Endpunkt zugewiesen ist, der als Scanner verwendet werden kann.

Neben den Standard-Scan-Aufgaben (die Sie nicht löschen oder kopieren können) können Sie beliebig viele benutzerdefinierte (Netzwerk-)Scan-Aufgaben erstellen.

Um eine neue benutzerdefinierte (Netzwerk-)Scan-Aufgabe zu erstellen und zu konfigurieren, klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** auf der rechten Seite der Tabelle. Um die Einstellungen für eine bestehende Scan-Aufgabe zu ändern, klicken Sie auf den Namen der entsprechenden Aufgabe. Bitte rufen Sie das folgende Thema auf, um mehr über die Konfiguration der Aufgabeneinstellungen zu erfahren.

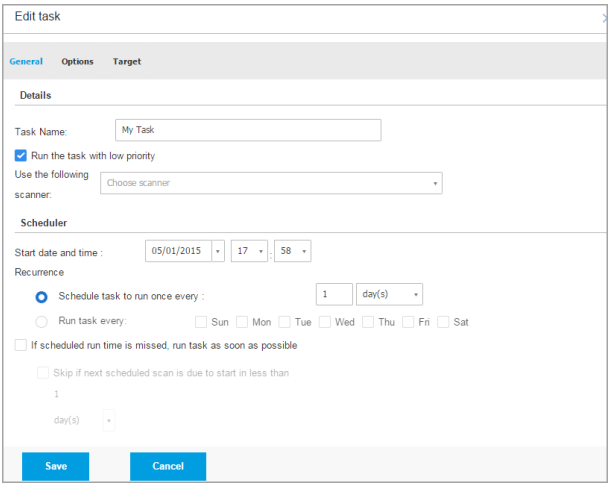
Um eine Aufgabe aus der Liste zu entfernen, klicken Sie auf die Schaltfläche ⊖ **Löschen** auf der rechten Seite der Tabelle.

Konfiguration einer Prüfaufgabe

Die Einstellungen für die Scan-Aufgaben sind auf drei Reiter verteilt:

- **Allgemein**: Aufgabenname und Zeitplanung festlegen.
- **Optionen**: Scan-Profil für eine schnelle Konfiguration der Scan-Einstellungen auswählen und Einstellungen für benutzerdefinierte Scans festlegen.
- **Ziel**: Hier können Sie die Dateien und Ordner auswählen, die gescannt werden sollen, und solche definieren, die vom Scan ausgeschlossen werden sollen.

Im Folgenden werden die Optionen vom ersten bis zum letzten Reiter beschrieben:



Richtlinien - Konfiguration der allgemeinen Einstellungen für Bedarf-Scan-Aufgaben

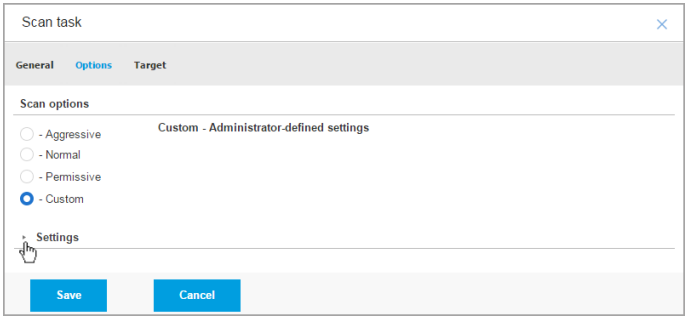
- **Details.** Geben Sie der Aufgabe einen eindeutigen Namen, der ihren Inhalt widerspiegelt. Wenn Sie einen Namen festlegen, berücksichtigen Sie das Ziel der Scan-Aufgabe und unter Umständen auch die Scan-Einstellungen.
- **Planer.** Verwenden Sie die Planungsoptionen, um den Scan-Zeitplan zu konfigurieren. Sie können festlegen, dass der Scan alle paar Stunden, Tage oder Wochen durchgeführt wird und Datum und Zeit des ersten Scans bestimmen.

  Bitte beachten Sie, dass die Computer eingeschaltet sein müssen, wenn der Termin fällig ist. Eine geplante Scan-Aufgabe kann nicht ausgeführt werden, wenn die Maschine zu diesem Zeitpunkt nicht eingeschaltet ist, sich im Ruhezustand oder Energiesparmodus befindet oder wenn kein Benutzer angemeldet ist. In diesen Fällen wird der Scan bis zum nächsten Mal verschoben.

  Beachten Sie
  Der geplante Scan wird zur lokalen Zeit des Zielendpunkts ausgeführt. Wenn der geplante Scan zum Beispiel um 18:00 starten soll und der Endpunkt in einer anderen Zeitzone als das Control Center ist, wird der Scan um 18:00 Uhr (Endpunkt-Zeit) gestartet.

- **Scan-Optionen.** Klicken Sie auf die Sicherheitsstufe, die Ihren Ansprüchen entspricht (aggressiv, normal oder tolerant). Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.

  Je nach ausgewähltem Profil werden die Scan-Optionen im Bereich **Einstellungen** automatisch konfiguriert. Bei Bedarf können Sie diese aber auch im Detail konfigurieren. Markieren Sie dazu das Kästchen **Benutzerdefiniert** und gehen Sie dann zum Bereich **Einstellungen**.



Scan-Aufgabe - Konfiguration eines benutzerdefinierten Scans

- **Dateitypen.** Verwenden Sie diese Optionen, um festzulegen, welche Dateien gescannt werden sollen. Sie können Endpoint Security so einrichten, dass Scans durchgeführt werden für alle Dateien (unabhängig von der Dateiendung), nur für Anwendungsdateien oder nur für bestimmte Dateiendungen, die Sie für gefährlich erachten. Das Scannen aller Dateien bietet den besten Schutz, während das Scannen nur von Anwendungen verwendet wird, um einen schnelleren Scan durchzuführen.

  Beachten Sie

  Anwendungsdateien sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen. Weitere Informationen finden Sie unter „Anwendungsdateitypen“ (S. 176).

  Wenn Sie nur bestimmte Dateiendungen scannen lassen möchten, wählen Sie **Benutzerdefinierte Endungen** aus dem Menü, und geben Sie dann die Endungen in das Eingabefeld ein. Klicken Sie nach jeder Eingabe auf `Speichern`.

- **Archive.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für die Systemsicherheit. Die Malware kann das System nur beeinflussen, wenn die infizierten Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird. Wir empfehlen jedoch, diese Option zu nutzen, um jegliche potentiellen Bedrohungen aufzuspüren und zu entfernen, auch wenn es sich nicht um unmittelbare Bedrohungen handelt.

  Beachten Sie

  Das Scannen archivierter Dateien erhöht die Gesamt-Scandauer und erfordert mehr Systemressourcen.

  – **Inhalt von Archiven scannen.** Wählen Sie diese Option, wenn Sie archivierte Dateien nach Malware durchsuchen möchten. Sollten Sie sich zur Verwendung dieser Option entscheiden, können Sie die folgenden Optimierungsoptionen konfigurieren:

    - **Archivgröße begrenzen auf (MB).** Sie können Sie die maximale Größe der Archive angeben, die gescannt werden sollen. Markieren Sie das entsprechende Kästchen und geben Sie die maximale Archivgröße in MB ein.

    - **Maximale Archivtiefe (Ebenen).** Markieren Sie das entsprechende Kästchen und wählen Sie die maximale Archivtiefe aus dem Menü. Für

optimale Leistung wählen Sie den niedrigsten Wert, für maximalen Schutz wählen Sie den höchsten Wert.

- **E-Mail-Archive scannen.** Wählen Sie diese Option, wenn Sie möchten, dass E-Mail-Dateien und E-Mail-Datenbanken (Dateiformate wie EML, MSG, PST, DBX, MBX, TBB usw.) gescannt werden.

  Beachten Sie
  Das Scannen von E-Mail-Archiven kann viele Ressourcen beansprucht und die Systemleistung beeinträchtigen.

- **Verschiedenes.** Markieren Sie die entsprechenden Kästchen, um die gewünschten Scan-Optionen zu aktivieren.
  - **Boot-Sektoren scannen.** Prüft die Bootsektoren des Systems. Dieser Sektor der Festplatte beinhaltet den notwendigen Code um den Boot-Prozess zu starten. Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.
  - **Registry scannen.** Wählen Sie diese Option, um die Registry-Schlüssel zu scannen. Die Windows-Registry ist eine Datenbank, in der Konfigurationseinstellungen und Optionen für die Windows-Betriebssystemkomponenten sowie für die installierten Anwendungen gespeichert sind.
  - **Nach Rootkits suchen.** Wählen Sie diese Option, um nach Rootkits und Objekten zu suchen, die mit dieser Art von Software versteckt werden.
  - **Nach Keyloggern suchen.** Wählen Sie diese Option, wenn nach Keylogger-Software gesucht werden soll.
  - **Speicher scannen.** Wählen Sie diese Option, um Programme zu scannen, die im Speicher des Systems laufen.
  - **Cookies scannen.** Wählen Sie diese Option, um die Cookies zu scannen, die von Browsern auf dem Endpunkt gespeichert werden.
  - **Nur neue und geänderte Dateien.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
  - **Nach potenziell unerwünschten Anwendungen (PUA) scannen.** Eine potenziell unerwünschte Anwendung (PUA) ist ein Programm, das auf dem PC

vermutlich nicht erwünscht ist und häufig in Verbindung mit Freeware installiert wurde. Diese Art von Programmen kann ohne Zustimmung des Benutzers installiert werden (wird auch als Adware bezeichnet) oder wird standardmäßig bei der Express-Installation mitinstalliert (werbeunterstützt). Diese Programme können Pop-up-Werbung anzeigen, unerwünschte Symbolleisten im Standard-Browser installieren oder Hintergrundprozesse ausführen und so den PC verlangsamen.

- **Aktionen.** Abhängig vom gefundenen Dateityp werden folgende Aktionen automatisch ausgeführt:
  - **Standardaktion für infizierte Dateien.** Als infiziert eingestufte Dateien stimmen mit einer Malware-Signatur der Bitdefender Malware-Signaturen-Datenbank überein. Endpoint Security kann normalerweise den Malware-Code aus einer infizierten Datei entfernen und die ursprüngliche Datei rekonstruieren. Diesen Vorgang bezeichnet man als Desinfektion.

    Wenn eine infizierte Datei gefunden wird, versucht Endpoint Security automatisch, diese zu desinfizieren. Falls die Desinfizierung fehlschlägt, wird die Datei in die Quarantäne verschoben, um dort die Infizierung einzudämmen.

    Wichtig
    Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

  - **Standardaktion für verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert. Da es sich bei B-HAVE um eine heuristische Analysetechnologie handelt, kann Endpoint Security nicht sicher sein, ob die Datei tatsächlich mit Malware infiziert ist. Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.

    Scan-Aufgaben sind standardmäßig so konfiguriert, dass verdächtigte Dateien ignoriert werden. Es könnte ratsam sein, die Standardaktion zu ändern, damit verdächtige Dateien in Quarantäne verschoben werden. Dateien in Quarantäne werden zu Analysezwecken in regelmäßigen Abständen an die Bitdefender-Labs geschickt. Sollten das Vorhandensein von Malware

bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

– **Standardaktion für Rootkits.** Rootkits sind spezielle Software-Wekzeuge, die verwendet werden, um Dateien vor dem Betriebssystem zu verbergen. Obwohl sie nicht zwangsläufig als schädlich anzusehen sind, werden Rootkits häufig genutzt, um Malware zu verbergen oder Eindringlinge im System zu tarnen.

  Erkannte Rootkits und versteckte Dateien werden standardmäßig ignoriert.

Sie können die standardmäßigen Aktionen verändern, dies wird aber nicht empfohlen. Sie können eine zweite Aktion auswählen, für den Fall, dass die Erste fehlschlägt und außerdem verschiedene Aktionen für jede Kategorie. Wählen Sie aus den entsprechenden Menus die erste und zweite Aktion, die für jeden entdeckten Dateityp vorgenommen werden soll. Folgende Aktionen stehen zur Verfügung:

Keine Aktion ausführen
Für gefundene Dateien wird keine Aktion durchgeführt. Diese Dateien werden nur in das Scan-Protokoll aufgenommen.

Desinfizieren
Den Malware-Kode aus den entdeckten infizierten Dateien entfernen. Es wird empfohlen, dass dies immer die erste Aktion bleibt, die für infizierte Dateien durchgeführt wird.

Löschen
Infizierte Dateien ohne vorherige Benachrichtigung von der Festplatte löschen. Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.

Dateien in Quarantäne verschieben
Verschieben Sie infizierte Dateien von ihrem Speicherort in den Quarantäne-Ordner. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. Sie können die Dateien in Quarantäne über die Quarantäne-Seite in der Konsole verwalten.

- **Scan-Ziel.** Fügen Sie der Liste alle Pfade hinzu, die auf den Ziel-Computern gescannt werden sollen.

  Um eine neue Datei oder einen neuen Ordner zum Scan hinzuzufügen:

  1. Wählen Sie einen vorgegebenen Speicherort aus dem Klappmenü, oder geben Sie **Bestimmte Pfade** ein, die sie scann lassen möchten.

2. Geben Sie den Pfad des zu scannenden Objekts im Bearbeitungsfeld ein.
   - Wenn Sie einen vorgegebenen Pfad ausgewählt haben, vervollständigen Sie den Pfad nach Bedarf. Um zum Beispiel den gesamten Ordner `Programme` zu scannen, müssen Sie lediglich den entsprechenden vorgegebenen Pfad aus dem Klappmenü auswählen. Um einen bestimmten Order im Ordner `Programme` zu scannen, müssen Sie den Pfad vervollständigen indem Sie einen Backslash (\) und den Namen des Ordners hinzufügen.
   - Wenn Sie **Bestimmte Pfade** ausgewählt haben, geben Sie den vollständigen Pfad des Objektes ein, das gescannt werden soll. Es empfiehlt sich, (nach Möglichkeit) Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist.
3. Klicken Sie auf den entsprechenden ⊕ **Hinzufügen**-Link.

   Um einen bestehenden Pfad zu bearbeiten, klicken Sie ihn an. Um einen Server aus der Liste zu entfernen, bewegen Sie den Mauszeiger darüber, und klicken Sie auf die entsprechende ⊖ **Löschen**-Schaltfläche.

- Für Netzwerk-Scan-Aufgaben müssen Sie die Zugangsdaten eines Benutzerkontos mit Lese- und Schreibberechtigung auf den entsprechenden Netzwerklaufwerken eingeben, damit der Sicherheitsagent auf diese Netzwerklaufwerke zugreifen und die entsprechenden Aktionen durchführen kann.
- **Ausschlüsse.** Sie können entweder die im Bereich **Malware-Schutz > Ausschlüsse** der aktuellen Richtlinie definierten Ausschlüsse verwenden oder für die aktuelle Scan-Aufgabe benutzerdefinierte Ausschlüsse definieren. Weitere Informationen finden Sie unter „Ausschlüsse“ (S. 101).

Geräte-Scan

Sie können festlegen, dass Endpoint Security externe Speichermedien automatisch erkennt und scannt, sobald diese mit dem Endpunkt verbunden werden. Entdeckte Geräte fallen in eine dieser Kategorien:

- CDs/DVDs
- USB-Speichergeräte, sowie Flashstifte und externe Festplatten
- Zugeordnete Netzlaufwerke
- Geräte mit mehr als einer bestimmten Menge gespeicherter Daten.

Bei den Geräte-Scans werden als infiziert erkannte Dateien automatisch desinfiziert oder, falls eine Desinfektion nicht möglich ist, in die Quarantäne verschoben. Bitte beachten Sie, dass für infizierte Dateien auf CDs/DVDs oder auf zugeordneten Netzlaufwerken mit schreibgeschütztem Zugriff keine Aktionen durchgeführt werden können.

Beachten Sie
Der Benutzer kann während eines Geräte-Scans weiterhin auf alle Daten auf dem Gerät zugreifen.

Wenn Warnfenster unter **Allgemein > Anzeige** aktiviert wurden, wird der Benutzer zunächst gefragt, ob ein erkanntes Gerät gescannt werden soll. Es erfolgt kein automatischer Scan.

Wenn ein Geräte-Scan beginnt:

- Ein Benachrichtigungsfenster informiert den Benutzer über den Geräte-Scan, vorausgesetzt das Benachrichtigungsfenster unter **Allgemein > Anzeige** aktiviert wurden.

Nach Abschluss des Scans muss der Benutzer eventuell erkannte Bedrohungen überprüfen.

Wählen Sie die **Geräte-Scan**-Option, um die automatische Erkennung und Prüfung von Speichergeräten zu aktivieren. Mit den folgenden Optionen können Sie den Geräte-Scan für jeden Gerätetyp individuell festlegen:

- **CD-/DVD-Datenträger**
- **USB-Speichergeräte**
- **Zugeordnete Netzlaufwerke**
- **Keine Geräte scannen, die mehr Daten gespeichert haben als (MB)**. Mit dieser Option können Sie die Scans von erkannten Geräten automatisch überspringen, wenn die darauf gespeicherten Daten einen festgelegten Umfang überschreiten. Geben Sie das Grössenlimit (in MB) in das entsprechende Feld ein. Null bedeutet, dass kein Grössenlimit angegeben wurde.

  Beachten Sie
  Diese Option betrifft nur CDs/DVDs und USB Speichergeräte.

Einstellungen

In diesem Bereich können Sie die Quarantäne-Einstellungen und die Regeln für Scan-Ausschlüsse festlegen.

- Quarantäne-Einstellungen konfigurieren
- Konfiguration der Scan-Ausschlüsse

Quarantäne

Für die von den Zielendpunkten in die Quarantäne verschobenen Dateien können Sie die folgenden Optionen konfigurieren:

- **Delete files older than (days).** Standardmäßig werden Dateien in der Quarantäne, die älter als 30 Tage sind, automatisch gelöscht. Um dieses Intervall zu ändern, wählen Sie im Menü eine andere Option aus.
- **Quarantäne-Dateien an das Bitdefender-Labor senden, jeweils alle (Stunden).** Standardmäßig werden in die Quarantäne verschobene Dateien automatisch stündlich an die Bitdefender-Labors gesandt. Sie können das Intervall einstellen, in dem in die Quarantäne verschobene Dateien gesendet werden (standardmäßig 1 Stunde). Die Beispieldateien werden dann von den Bitdefender-Malware-Forschern analysiert. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.
- **Quarantäne nach Signaturen-Update erneut scannen.** Lassen Sie diese Option aktiviert, um Dateien in Quarantäne automatisch nach jedem Update der Malware-Signaturen zu scannen. Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt.
- **Dateien vor der Desinfektion in die Quarantäne kopieren.** Aktivieren Sie diese Option, um im Falle von Fehlalarmen Datenverlust zu vermeiden, indem als infiziert erkannte Dateien vor der Desinfektion in die Quarantäne kopiert werden. Später können Sie unbedenkliche Dateien von der Seite **Quarantäne** aus wiederherstellen.

Ausschlüsse

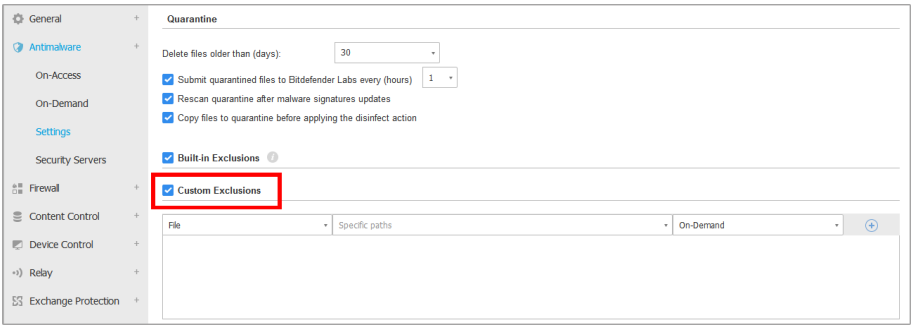
Der Bitdefender-Sicherheitsagent kann bestimmte Objekttypen vom Scan ausschließen. Sie können bei Bedarf auch selbst weitere Ausschlüsse definieren. In diesem Bereich können Sie die Verwendung verschiedener Arten von Ausschlüssen im Bitdefender-Sicherheitsagent konfigurieren.

- **Eingebaute Ausschlüsse** sind standardmäßig aktiviert und im Bitdefender-Sicherheitsagenten enthalten.

  Wenn Sie alle Objekttyen scannen möchten, können Sie eingebaute Ausschlüsse deaktivieren, dies wird sich aber erheblich auf die Leistung der Maschine und die Dauer des Scans auswirken.

- Wenn Sie bestimmte Objekte vom Scan ausschließen möchten, können Sie die Option **Benutzerdefinierte Ausschlüsse** aktivieren und die Ausschlüsse ganz nach Bedarf konfigurieren.

  Ausschlüsse können auf Zugriff-Scans, Bedarf-Scans oder beide Scan-Arten angewendet werden. Je nach ausgeschlossenem Objekt gibt es vier Ausschlussarten:



Richtlinien - Benutzerdefinierte Ausschlüsse

  - **Dateiausschlüsse:** Nur die angegebene Datei wird vom Scan ausgeschlossen.
  - **Ordnerausschlüsse:** Alle Dateien in dem angegebenen Ordner und alle Unterordner werden vom Scan ausgeschlossen.
  - **Ausschlüsse für Dateiendungen:** Alle Dateien mit der angegebenen Dateiendung werden vom Scan ausgeschlossen.
  - **Prozessausschlüsse:** Jedes Objekt, auf das von dem ausgeschlossenen Prozess zugegriffen wird, wird ebenfalls vom Scan ausgeschlossen. Sie können auch für Active Virus Control und das Angriffserkennungssystem (IDS) Prozessausschlüsse festlegen.

Wichtig

Scan-Ausschlüsse sollten unter besonderen Umständen eingesetzt werden oder wenn dies von Microsoft oder Bitdefender empfohlen wird. Eine aktualisierte Liste der von Microsoft empfohlenen Ausschlüsse finden Sie in diesem Artikel. Sollten Sie eine EICAR-Testdatei verwenden, um den Malware-Schutz regelmäßig zu überprüfen, sollten Sie diese von den Zugriff-Scans ausschließen.

So konfigurieren Sie eine benutzerdefinierte Ausschlussregel:

1. Wählen Sie die Art des Ausschlusses aus dem Menü.
2. Je nach Ausschlussart geben Sie das auszuschließende Objekt wie folgt an:
   - **Datei-, Ordner- und Prozessausschlüsse.** Sie müssen den Pfad des ausgeschlossenen Objekts auf den Ziel-Computern angeben.
     a. Sie können entweder einen vorgegebenen Pfad aus dem Menü wählen oder einen bestimmten Pfad eingeben.
     b. Wenn Sie einen vorgegebenen Pfad ausgewählt haben, vervollständigen Sie den Pfad nach Bedarf. Um zum Beispiel den gesamten Ordner `Programme` auszuschließen, müssen Sie lediglich den entsprechenden vorgegebenen Pfad aus dem Menü auswählen. Um einen bestimmten Order im Ordner `Programme` auszuschließen, müssen Sie den Pfad vervollständigen indem Sie einen Backslash (\) und den Namen des Ordners hinzufügen. Bei Prozessausschlüssen müssen Sie auch den Namen der ausführbaren Datei der Anwendung angeben.
     c. Wenn Sie einen bestimmten Pfad hinzufügen möchten, geben Sie den vollständigen Pfad des Objektes ein, das ausgeschlossen werden soll. Es empfiehlt sich, (nach Möglichkeit) Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist.
   - **Ausschlüsse für Dateiendungen.** Geben Sie mindestens eine Dateiendung ein (Mehrfachnenneungen mit Semikolon ";" getrennt), die vom Scan ausgeschlossen werden sollen. Sie können die Endungen dabei mit oder ohne den führenden Punkt eingeben. Geben Sie zum Beispiel die Endung `txt` ein, um Textdateien auszuschließen.

Beachten Sie
Bevor Sie Dateiendungen ausschließen, sollten Sie sich eingehend darüber informieren, welche Endungen häufig im Visier von Malware stehen und welche nicht.

3. Wählen Sie die Scan-Arten aus, für die die Regel angewendet werden soll. Einige Ausschlüsse sind möglicherweise nur für Zugriff-Scans von Bedeutung, einige wiederum nur für Bedarf-Scans und andere empfehlen sich unter Umständen für beide Arten von Scans.

   Sie können für die Zugriff-Scans, Active Virus Control und das Angriffserkennungssystem (IDS) Prozessausschlüsse festlegen.

   Wichtig
   Bitte beachten Sie, dass Ausschlüsse für Bedarf-Scans bei Kontext-Scans NICHT berücksichtigt werden. Klicken Sie mit der rechten Maustaste auf eine Datei oder einen Ordner und wählen Sie **Mit Bitdefender Endpoint Security Tools scannen**, um einen Kontext-Scan zu starten.

4. Klicken Sie auf den Button ⊕**Hinzufügen**. Die neue Regel wird der Liste hinzugefügt.

Um eine Regel aus der Liste zu löschen, klicken Sie auf den entsprechenden ⊗ **Löschen**-Link.

5.2.3. Firewall

Die Firewall schützt der Endpunkt vor nicht autorisierten Zugriffsversuchen bei eingehendem und ausgehendem Datentransfer.

Die Funktionsweise der Firewall basiert auf Netzwerkprofilen. Die Profile wiederum basieren auf Vertrauensstufen, die für jedes Netzwerk definiert werden müssen.

Die Firewall erkennt jede neue Verbindung, gleich die Informationen des Netzwerkadapters dieser Verbindung mit den Informationen der bestehenden Profile ab und wendet das entsprechende Profil an. Nähere Informationen zur Anwendung der Profile finden Sie unter „Netzwerkeinstellungen“ (S. 107).

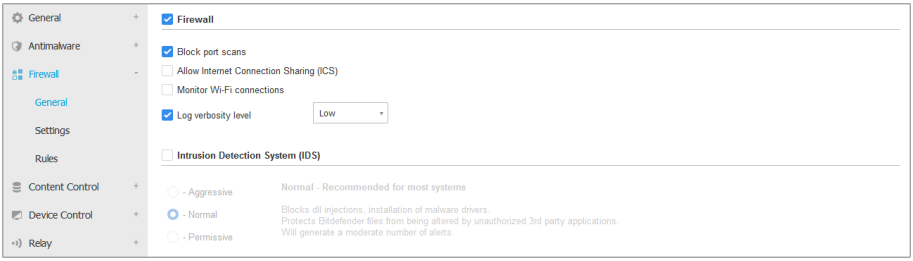
Wichtig
Das Firewall-Modul steht nur für Windows-Arbeitsplätze zur Verfügung.

Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- Allgemein
- Einstellungen
- Regeln

Allgemein

In diesem Bereich können Sie die Bitdefender-Firewall aktivieren und deaktivieren und die allgemeinen Einstellungen konfigurieren.



Richtlinien - Allgemeine Firewall-Einstellungen

- **Firewall.** Über das Kästchen können Sie die Firewall aktivieren oder deaktivieren.

  Warnung
  Wenn Sie den Firewall-Schutz deaktivieren, werden die Computer anfällig für Angriffe über das Netzwerk und das Internet.

- **Port-Scans blockieren.** Portscans werden von Hackern verwendet, um herauszufinden, welche Ports auf einem Computer geöffnet sind. Wenn Sie dann einen unsicheren Port finden, können Sie in den Computer eindringen.
- **Gemeinsame Nutzung der Internetverbindung (ICS) zulassen.** Wählen Sie diese Option, damit die Firewall die gemeinsame Nutzung der Internetverbindung zulässt.

  Beachten Sie
  Diese Option aktiviert nicht automatisch die gemeinsame Nutzung der Internetverbindung (Internet Connection Sharing) auf dem Computer des Benutzers.

- **WLAN-Verbindungen überwachen.** Der Bitdefender-Sicherheitsagent kann Benutzer in einem Drahtlosnetzwerk über neu zum Netzwerk hinzugekommene Computer informieren. Wählen Sie diese Option aus, um solche Benachrichtigungen auf dem Bildschirm des Benutzers anzuzeigen.
- **Ausführlichkeitsstufe Protokoll.** Der Bitdefender-Sicherheitsagent erstellt ein Protokoll der Ereignisse, die im Zusammenhang mit der Nutzung des Firewall-Moduls auftreten (Aktivieren/Deaktivieren der Firewall, Blockieren des Datenverkehrs, Einstellungsänderungen) oder die durch Aktivitäten erzeugt wurden, die von diesem Modul erkannt wurden (Port-Scans, regelbasiertes Blockieren von Verbindungsversuchen und Datenverkehr). Wählen Sie unter **Ausführlichkeitsstufe Protokoll** eine Option aus, um festzulegen, wie viele Informationen im Protokoll enthalten sein sollen.
- **Angriffserkennungssystem (IDS).** Das Angriffserkennungssystem (IDS) überwacht das System und sucht nach verdächtigen Aktivitäten (so zum Beispiel unerlaubte Versuche, Bitdefender-Dateien zu verändern, DLLs einzuschleusen, Tastaturanschläge zu protokollieren, etc.).

  Um das Angriffserkennungssystem (IDS) zu konfigurieren:

  1. Über das Kästchen können Sie das Angriffserkennungssystem (IDS) aktivieren oder deaktivieren.
  2. Klicken Sie auf die Sicherheitsstufe, die Ihren Ansprüchen entspricht (aggressiv, normal oder tolerant). Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.

  Um zu verhindern, dass eine harmlose Anwendung vom Angriffserkennungssystem erkannt wird, fügen Sie eine **AVC/IDS-Prozessausschlussregel** für diese Anwendung im Bereich **Malware-Schutz > Einstellungen > Benutzerdefinierte Ausschlüsse** hinzu.

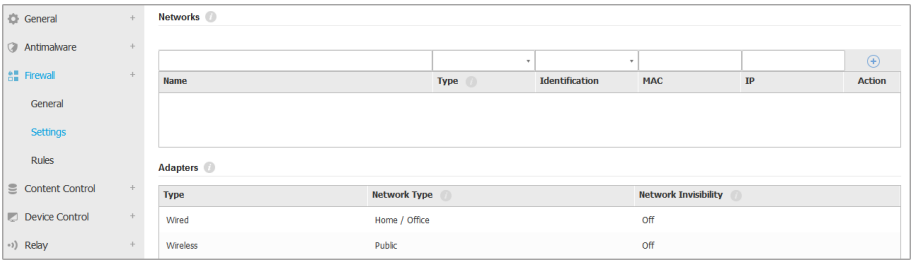
Einstellungen

Je nach Vertrauensstufe wendet die Firewall automatisch ein Profil an. Verschiedene Netzwerkverbindungen können unterschiedliche Vertrauensstufen haben, je nach Architektur des Netzwerk oder Art des Adapters, über den die Verbindung hergestellt wird. Wenn Sie zum Beispiel Teilnetzwerke in Ihrem Unternehmensnetzwerk haben, können Sie für jedes Teilnetzwerk eine eigene Vertrauensstufe festlegen.

Die Einstellungen sind in den folgenden Tabellen sortiert:

- Netzwerke

- Adapter



Richtlinien - Firewall Einstellungen

Netzwerkeinstellungen

Wenn Sie möchten, dass die Firewall verschiedenen Bereichen Ihres Unternehmens unterschiedliche Profile zuweist, müssen Sie die verwalteten Netzwerke in der Tabelle **Netzwerke** angeben. Füllen Sie die Felder der Tabelle **Netzwerke** wie folgt aus:

- **Name.** Geben Sie einen aussagekräftigen Namen für das Netzwerk ein.
- **Typ.** Hier können Sie aus dem Menü die Art des Profils wählen, das dem Netzwerk zugewiesen wird.

  Der Bitdefender-Sicherheitsagent wendet automatisch eins der vier Netzwerk-Profile auf jede erkannte Netzwerkverbindung des Endpunkts an, um die grundlegenden Datenverkehrfilteroptionen festzulegen. Es gibt folgende Profiltypen:

  - **Vertrauenswürdiges** Netzwerk. Deaktiviert die Firewall für die entsprechenden Adapter.
  - **Heim-/Büronetzwerk**. Lässt sämtlichen Datenverkehr zwischen den Computern im lokalen Netzwerk zu; anderer Datenverkehr wird gefiltert.
  - **Öffentliches** Netzwerk. Sämtlicher Datenverkehr wird gefiltert.
  - **Nicht vertrauenswürdiges** Netzwerk. Der Netzwerk- und Internet-Datenverkehr über die entsprechenden Adapter wird vollständig blockiert.
- **Identifikation.** Wählen Sie aus dem Menü die Methode, nach der der Bitdefender-Sicherheitsagent ein Netzwerk identifiziert. Es gibt drei Methoden zur identifizierung: **DNS**, **Gateway** und **Netzwerk**.

  - **DNS**: identifiziert alle Endpunkte über das angegebene DNS.
  - **Gateway**: identifiziert alle Endpunkte, die über das angegebene Gateway kommunizieren.
  - **Netzwerk**: identifiziert alle Endpunkte aus dem angegebenen Netzwerkbereich nach der entsprechenden Netzwerkadresse.
- **MAC**. In diesem Feld können Sie die MAC-Adresse eines DNS-Servers oder eines Gateways des Netzwerks angeben, je nach ausgewählter Identifikationsmethode.

  Die MAC-Adresse müssen Sie im Hexadezimalformat eingeben, durch Bindestriche (-) oder Doppelpunkte (:) getrennt. So sind z. B. sowohl `00-50-56-84-32-2b` als auch `00:50:56:84:32:2b` gültige Adressen.
- **IP.** In diesem Feld können Sie bestimmte IP-Adressen in einem Netzwerk definieren. Das Format der IP-Adresse hängt wie folgt von der Identifikationsmethode ab:
  - **Netzwerk.** Geben Sie die Netzwerknummer im CIDR-Format ein. Zum Beispiel `192.168.1.0/24`, wobei `192.168.1.0` die Netzwerkadresse ist und `/24` die Netzwerkmaske.
  - **Gateway.** Geben Sie die IP-Adresse des Gateways ein.
  - **DNS.** Geben Sie die IP-Adresse des DNS-Servers ein.

Nachdem Sie ein Netzwerk definiert haben, klicken Sie auf die Schaltfläche **Hinzufügen** auf der rechten Seite der Tabelle, um das Netzwerk der Liste hinzuzufügen.

Adaptereinstellungen

Wenn ein Netzwerk erkannt wird, das nicht in der Tabelle **Netzwerke** definiert ist, erkennt der Bitdefender-Sicherheitsagent die Art des Netzwerkadapters und wendet ein passendes Profil auf die Netzwerkverbindung an.

Die Felder der Tabelle **Adapter** werden folgend beschrieben:

- **Typ.** Zeigt die Art des Netzwerkadapters an. Der Bitdefender-Sicherheitsagent kann drei verschiedene vordefinierte Adaptertypen erkennen: **Kabelgebunden**, **Kabellos** und **Virtuell** (Virtuelles Privates Netzwerk).
- **Netzwerktyp.** Beschreibt das Netzwerkprofil, das einem bestimmten Adaptertyp zugewiesen ist. Die Netzwerkprofile sind im Abschnitt Netzwerkeinstellungen

beschrieben. Wenn Sie auf das Netzwerktypfeld klicken, können Sie die Einstellung ändern.

Wenn Sie **Windows entscheiden lassen** wählen, wendet der Bitdefender-Sicherheitsagent für jede neue Netzwerkverbindung, die erkannt wird, nachdem die Richtlinie angewendet wurde, ein Profil für die Firewall an, das auf der Netzwerkklassifikation in Windows basiert. Die Einstellungen der Tabelle **Adapter** werden dabei ignoriert.

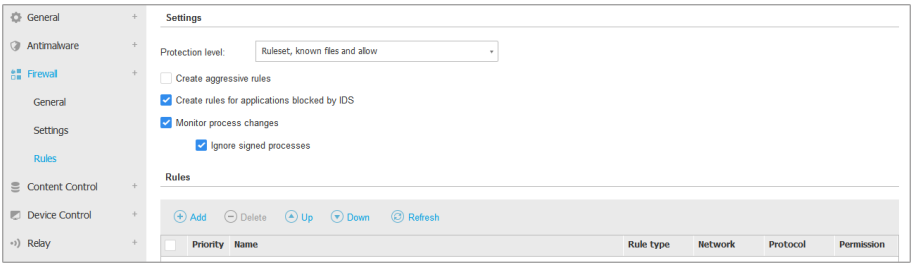
Wenn die Erkennung auf der Basis des Windows-Netzwerkmanagers fehlschlägt, wird eine einfache Erkennung versucht. Ein generisches Profil wird angewendet, in dem das Netzwerkprofil **Öffentlich** zugrundegelegt und die Tarnkappeneinstellung auf **Ein** gestellt wird.

Wenn die IP-Adresse der Domain, in der der Computer gefunden wurde, in einem der mit dem Adapter assoziierten Netzwerke liegt, wird die Vertrauensstufe **Heim/Büro** zugrundegelegt und die Tarnkappeneinstellungnstellung auf **Remote** gestellt. Wenn der Computer nicht in einer Domain ist, wird diese Bedingung ignoriert.

- **Netzwerk-Unsichtbarkeit.** Der Stealth-Modus macht Ihren Computer im Netzwerk oder Internet unsichtbar für schädliche Software und Hacker. Konfigurieren Sie die Netzwerk-Unsichtbarkeit nach Bedarf für jeden Adaptertypen, indem Sie jeweils eine der folgenden Optionen auswählen:
  - **An.** Der Computer ist sowohl im lokalen Netzwerk als auch im Internet unsichtbar.
  - **Aus.** Jeder Benutzer in lokalen Netzwerk oder dem Internet kann den Computer anpingen oder erkennen.
  - **Remote.** Der Computer kann nicht über das Internet erkannt werden. Jeder Benutzer im lokalen Netzwerk kann den Computer anpingen oder erkennen.

Regeln

In diesem Bereich können Sie den Netzwerkzugriff für Anwendungen und die Firewall-Regeln für den Datenverkehr festlegen. Bitte beachten Sie, dass die verfügbaren Einstellungen nur auf die **Heim/Büro**- oder **Öffentlichen** Profile angewendet werden können.



Richtlinien - Firewall-Regeleinstellungen

Einstellungen

Sie können die folgenden Einstellungen vornehmen:

- **Sicherheitsstufe.** Die ausgewählte Sicherheitsstufe definiert die Firewall-Entscheidungslogik, die verwendet wird, wenn Anwendungen den Zugriff auf Netzwerk- oder Internet-Dienste anfordern. Die folgenden Optionen sind verfügbar:

  Bestehende Regeln, sonst zulassen
  Bestehende Firewall-Regeln anwenden und alle weiteren Verbindungsversuche automatisch zulassen. Für jeden neuen Verbindungsversuch wird eine Regel angelegt und zum Regelsatz hinzugefügt.

  Bestehende Regeln und nachfragen
  Bestehende Firewall-Regeln anwenden und den Benutzer für alle weiteren Verbindungsversuche zur Auswahl einer Aktion auffordern. Ein Warnfenster mit detaillierten Informationen über den unbekannten Verbindungsversuch wird auf dem Bildschirm des Benutzers angezeigt. Für jeden neuen Verbindungsversuch wird eine Regel angelegt und zum Regelsatz hinzugefügt.

  Bestehende Regeln, sonst verweigern
  Bestehende Firewall-Regeln anwenden und alle weiteren Verbindungsversuche automatisch verweigern. Für jeden neuen Verbindungsversuch wird eine Regel angelegt und zum Regelsatz hinzugefügt.

Bestehende Regeln, bekannte Dateien, sonst zulassen
Bestehende Firewall-Regeln anwenden, die Verbindungsversuche von bekannten Anwendungen automatisch zulassen und alle weiteren unbekannten Verbindungsversuche automatisch zulassen. Für jeden neuen Verbindungsversuch wird eine Regel angelegt und zum Regelsatz hinzugefügt.

Bestehende Regeln, bekannte Dateien und nachfragen
Bestehende Firewall-Regeln anwenden, die Verbindungsversuche von bekannten Anwendungen automatisch zulassen und den Benutzer für alle weiteren unbekannten Verbindungsversuche zur Auswahl einer Aktion auffordern. Ein Warnfenster mit detaillierten Informationen über den unbekannten Verbindungsversuch wird auf dem Bildschirm des Benutzers angezeigt. Für jeden neuen Verbindungsversuch wird eine Regel angelegt und zum Regelsatz hinzugefügt.

Bestehende Regeln, bekannte Dateien, sonst verweigern
Bestehende Firewall-Regeln anwenden, die Verbindungsversuche von bekannten Anwendungen automatisch zulassen und alle weiteren unbekannten Verbindungsversuche automatisch verweigern. Für jeden neuen Verbindungsversuch wird eine Regel angelegt und zum Regelsatz hinzugefügt.

Beachten Sie
Bekannte Dateien sind eine Sammlung von sicheren und vertrauenswürdigen Anwendungen, die von Bitdefender zusammengestellt und fortlaufend gepflegt wird.

- **Aggressive Regeln erstellen.** Wenn diese Option aktiviert ist, werden für jeden Prozess, der die Anwendung öffnet, die Zugriff auf das Netzwerk oder das Internet anfordert, von der Firewall Regeln erstellt.
- **Erstellen Sie Regeln für Anwendungen, die durch das IDS blockiert werden.** Wenn diese Option ausgewählt ist, erstellt die Firewall jedes Mal, wenn das Angriffserkennungssystem eine Anwendung blockiert, automatisch eine **Verweigern**-Regel.
- **Prozessänderungen überwachen.** Wählen Sie diese Option, wenn Sie möchten, dass jede Anwendung, die sich mit dem Internet verbinden möchte, darauf überprüft wird, ob sie seit der Festlegung der Regel für ihren Internetzugriff

verändert wurde. Falls die Anwendung geändert wurde, wird eine neue Regel in Übereinstimmung mit dem aktuellen Sicherheitsstufe angelegt.

Beachten Sie

Normalerweise werden Anwendungen durch Updates verändert. Es kann aber auch sein, dass eine Anwendung durch Malware verändert wird um den lokalen Computer oder andere Computer in dem Netzwerk zu infizieren.

Signierte Anwendungen sind in normalerweise vertrauenswürdig und haben einen höheren Sicherheitsgrad. Wählen Sie **Signierten Prozess ignorieren**, um veränderten signierten Anwendungen automatisch die Verbindung mit dem Internet zu erlauben.

Regeln

In der Regeltabelle werden die aktuellen Firewall-Regeln mit wichtigen Informationen zu den einzelnen Regel angezeigt:

- Name der Regel oder Anwendung, auf die sie sich bezieht.
- Protokoll, auf das die Regel angewendet werden soll.
- Aktion der Regel (Pakete zulassen oder verweigern).
- Für die Regel verfügbare Aktionen.
- Regelpriorität.

Beachten Sie

Diese Firewall-Regeln werden ausdrücklich von der Richtlinie umgesetzt. Zusätzliche Regeln werden unter Umständen auf Computern als Folge der Anwendung von Firewall-Einstellungen konfiguriert.

Eine Reihe von Standardregeln für die Firewall helfen Ihnen dabei, häufig genutzte Datenverkehrstypen ohne viel Aufwand zuzulassen oder zu verweigern. Wählen Sie die gewünschte Option aus dem **Berechtigung**-Menü.

Eingehende ICMP / ICMPv6

ICMP- / ICMPv6-Nachrichten zulassen oder verweigern. ICMP-Nachrichten werden häufig von Hackern für Angriffe auf Computer-Netzwerke genutzt. Standardmäßig wird diese Art Datenverkehr nicht zugelassen.

Eingehende Remote-Desktop-Verbindungen
Den Zugriff anderer Computer über Remote-Desktop-Verbindungen zulassen oder verweigern. Standardmäßig wird diese Art Datenverkehr zugelassen.

E-Mails versenden
Versand von E-Mails über SMTP zulassen oder verweigern. Standardmäßig wird diese Art Datenverkehr zugelassen.

Web-Browsing HTTP
HTTP-Browsing zulassen oder verweigern. Standardmäßig wird diese Art Datenverkehr zugelassen.

In einem anderen Netzwerk drucken
Den Zugriff auf Drucker in anderen lokalen Netzwerken erlauben oder verweigern. Standardmäßig wird diese Art Datenverkehr nicht zugelassen.

Windows-Explorer-Datenverkehr auf HTTP / FTP
HTTP- und FTP-Datenverkehr aus Windows Explorer heraus zulassen oder verweigern. Standardmäßig wird diese Art Datenverkehr nicht zugelassen.

Neben den Standardregeln können Sie weitere Firewall-Regeln für andere auf den Endpunkten installierte Anwendungen erstellen. Diese Konfiguration bleibt jedoch Administratoren vorbehalten, die über umfangreiche Netzwerkkenntnisse verfügen.

Um eine neue Regel zu erstellen und zu konfigurieren, klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** am rechten Rand der Tabelle. Weitere Informationen finden Sie hier.

Um eine Regel aus der Liste zu entfernen, wählen Sie sie aus und klicken Sie auf die Schaltfläche ⊖ **Löschen** am oberen Rand der Tabelle.

Beachten Sie
Sie können die Standard-Firewall-Regeln weder löschen noch bearbeiten.

Benutzerdefinierte Regeln konfigurieren

Sie können zwei Arten von Firewall-Regeln konfigurieren:

- **Anwendungsbasierte Regeln.** Diese Regeln gelten für bestimmte Programme auf den Client-Computern.
- **Verbindungbasierte Regeln.** Diese Regeln gelten für alle Anwendungen oder Dienste, die eine bestimmte Verbindung nutzen.

Um eine neue Regel zu erstellen und zu konfigurieren, klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** am oberen Rand der Tabelle, und wählen Sie den gewünschten Regeltyp aus dem Menü. Um eine bestehende Regel zu bearbeiten, klicken Sie auf den Namen der Regel.

Die folgenden Einstellungen können konfiguriert werden:

- **Name der Regel.** Geben Sie den Namen ein, unter dem die Regel in der Regeltabelle aufgeführt werden soll (so zum Beispiel den Namen der Anwendung, auf die die Regel angewendet wird).
- **Anwendungspfad** (nur für anwendungsbasierte Regeln). Sie müssen den Pfad der ausführbaren Anwendungsdatei auf den Ziel-Computern angeben.
  - Wählen Sie einen vorgegebenen Pfad aus dem Menü und vervollständigen Sie den Pfad nach Bedarf. So müssen Sie für eine Anwendung, die im Ordner `Programme` installiert ist, den Ordner `%Programme%` auswählen und den Pfad vervollständigen, indem Sie einen Backslash (\) und den Namen des Anwendungsordners hinzufügen.
  - Geben Sie den vollständigen Pfad in das Bearbeitungsfeld ein. Es empfiehlt sich, (nach Möglichkeit) Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist.
- **Befehlszeile** (nur für anwendungsbasierte Regeln). Wenn die Regel nur angewendet werden soll, wenn die ausgewählte Anwendung mit einem bestimmten Befehl in der Windows-Befehlszeile geöffnet wird, geben Sie den entsprechenden Befehl in das Bearbeitungsfeld ein. Andernfalls lassen Sie das Feld frei.
- **Anwendungs-MD5** (nur für anwendungsbasierte Regeln). Wenn die Regel die Integrität der Dateidaten der Anwendung anhand des MD5-Hashcodes überprüfen soll, geben Sie ihn in das Bearbeitungsfeld ein. Lassen Sie das Feld ansonsten frei.
- **Lokale Adresse.** Geben Sie die lokale IP-Adresse und den Port an, auf den die Regel angewendet werden soll. Wenn Sie mehr als einen Netzwerkadapter haben, können sie die Markierung im Kästchen **Alle** aufheben und eine bestimmte IP-Adresse eingeben. Um Verbindungen über einen bestimmten Port oder Port-Bereich zu filtern, deaktivieren Sie das Kästchen **Alle** und geben Sie den gewünschten Port oder Port-Bereich in das entsprechende Feld ein.
- **Remote-Adresse.** Geben Sie die Remote-IP-Adresse und den Port an, auf den die Regel angewendet werden soll. Um den ein- und ausgehenden Datenverkehr

auf einem bestimmten Computer zu filtern, deaktivieren Sie das Kästchen **Alle** und geben Sie seine IP-Adresse ein.

- **Regel nur für direkt verbundene Computer anwenden.** Sie können den Zugriff anhand der MAC-Adresse filtern.
- **Protokoll.** Wählen Sie das IP-Protokoll, auf das die Regel angewendet werden soll.
  - Wenn Sie möchten, dass die Regel für alle Protokolle angewendet wird, wählen Sie **Alle**.
  - Wenn Sie möchten, dass die Regel für TCP-Protokolle angewendet wird, wählen Sie **TCP**.
  - Wenn Sie möchten, dass die Regel für UDP-Protokolle angewendet wird, wählen Sie **UDP**.
  - Wenn die Regeln für ein bestimmtes Protokoll gelten soll, wählen Sie das gewünschte Protokoll aus dem Menü **Sonstige**.

    Beachten Sie

    Die Nummern von IP-Protokollen werden von der Internet Assigned Numbers Authority (IANA) zugewiesen. Die komplette Liste zugewiesener Nummern von IP-Protokollen finden Sie unter http://www.iana.org/assignments/protocol-numbers.

- **Richtung.** Wählen Sie die Datenverkehrsrichtung an, auf die die Regel angewendet werden soll.

Richtung	Beschreibung
Ausgehend	Die Regel bezieht sich nur auf den ausgehenden Datenverkehr.
Eingehend	Die Regel bezieht sich nur auf den eingehenden Datenverkehr.
Beides	Die Regel findet in beiden Richtungen Anwendung.

- **IP-Version.** Wählen Sie die IP-Version (IPv4, IPv6 oder andere), auf die die Regel angewendet werden soll.

- **Netzwerk.** Wählen Sie den Netzwerktyp aus, auf den die Regel angewendet werden soll.
- **Berechtigung.** Wählen Sie eine der verfügbaren Berechtigungs-Optionen:

Berechtigung	Beschreibung
Zulassen	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen erlaubt.
Verweigern	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen verweigert.

Klicken Sie auf **Speichern**, um die Regel hinzuzufügen.

Ordnen Sie die Regeln, die Sie erstellt haben, mithilfe der Pfeile auf der rechten Seite der Tabelle nach ihrer Priorität. Je weiter oben eine Regel in der Liste steht, desto höher ist ihre Priorität.

5.2.4. Inhalts -Steuer.

Über das Inhaltssteuerungsmodul können Sie die gewünschten Einstellungen für Inhaltsfilter und Identitätsschutz für die Benutzeraktivität (Surfen, E-Mail und Software-Anwendungen) vornehmen. Sie können den Zugriff auf das Internet und bestimmte Anwendungen einschränken und Datenverkehr-Scans, Phishing-Schutz- und Identitätschutzregeln konfigurieren. Bitte beachten Sie, dass die Einstellungen für die Inhaltssteuerung auf alle Benutzer angewendet werden, die sich an den Ziel-Computern anmelden.

Wichtig
Das Inhaltssteuerungsmodul steht nur für Windows-Arbeitsplätze zur Verfügung.

Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- Datenverkehr
- Web
- Datenschutz
- Anwendungen

Datenverkehr

Hier können Sie Einstellungen zur Sicherheit des Datenverkehrs in den folgenden Bereichen vornehmen:

- Optionen
- Traffic-Scan
- Ausschlüsse für Datenverkehrs-Scans

Richtlinien - Inhaltssteuerung - Datenverkehr

Optionen

- **SSL scannen**. Wählen Sie diese Option, wenn der SSL-Datenverkehr (Secure Sockets Layer) von den Sicherheitsmodulen des Bitdefender-Sicherheitsagenten überprüft werden soll.
- **Browser-Symbolleiste anzeigen**. Die Bitdefender-Symbolleiste informiert Benutzer über die Bewertung der Webseiten, die sie aufrufen. Die Bitdefender-Symbolleiste ist anders als andere Browser-Symbolleisten. Sie fügt lediglich einen kleinen Dragger zu Ihrem Browser hinzu, der am oberen Rand jeder Webseite angezeigt wird. Mit einem Klick auf den Dragger öffnen Sie die Symbolleiste.

  Abhängig davon, wie Bitdefender die Webseite einstuft, wird eine der folgenden Bewertungen auf der linken Seite der Symbolleiste eingeblendet:

  – Die Nachricht "Diese Website ist nicht sicher" erscheint auf rotem Hintergrund.

  – Die Nachricht "Vorsicht ist geboten" erscheint auf orangefarbenem Hintergrund.

  – Die Nachricht "Diese Website ist sicher" erscheint auf grünem Hintergrund.

- **Browser-Suchberater.** Der Suchberater bewertet sowohl die Suchergebnisse von Google, Bing und Yahoo! als auch Links auf Facebook und Twitter, indem es ein Symbol vor jedem Ergebnis platziert. Verwendete Symbole und ihre Bedeutung:

  Sie sollten diese Webseite nicht aufrufen.
  Diese Webseite könnte gefährliche Inhalte haben. Seien Sie vorsichtig, wenn Sie sie dennoch aufrufen möchten.
  Diese Seite ist sicher.

Traffic-Scan

Eingehende E-Mails und der Internet-Datenverkehr werden in Echtzeit gescannt, um zu verhindern, dass Malware auf den Endpunkt heruntergeladen wird. Ausgehende E-Mails werden gescannt, um zu verhindern, dass Malware andere Endpunkte infiziert. Das Scannen des Web-Datenverkehrs kann Ihren Webbrowser geringfügig verlangsamen, dadurch können aber über das Internet übertragene Malware, einschließlich Drive-by-Downloads, blockiert werden.

Wenn eine infizierte E-Mail erkannt wird, wird diese automatisch mit einer Standard-E-Mail ersetzt, die den Empfänger über die ursprüngliche infizierte E-Mail informiert. Wenn eine Webseite Malware enthält oder verbreitet, wird diese automatisch blockiert. Anstelle der Webseite wird eine Warnung angezeigt, die den Anwender darüber informiert, das die aufgerufene Seite gefährlich ist.

Sie können zur Steigerung der Systemleistung das Scannen des E-Mail- und Internet-Datenverkehrs deaktivieren, dies wird aber nicht empfohlen. Dabei handelt es sich nicht um eine ernstzunehmende Bedrohung, solange die Zugriff-Scans für lokale Dateien aktiviert bleiben.

Ausschlüsse für Datenverkehrs-Scans

Wenn die Internet-Datenverkehr-Scan-Optionen aktiviert sind, können Sie bestimmte Arten von Datenverkehr vom Scan auf Malware ausschließen.

So definieren Sie einen Datenverkehr-Scan-Ausschluss:

1. Wählen Sie die Art des Ausschlusses aus dem Menü.
2. So definieren Sie je nach Ausschlusstyp die Datenverkehrsentität, die vom Scan ausgeschlossen werden soll:
   - **IP**. Geben Sie die IP-Adresse ein, deren eingehenden und ausgehenden Datenverkehr Sie nicht scannen möchten.

- **URL**. Schließt die eingegebenen Web-Adressen vom Scan aus. So definieren Sie einen URL-Scan-Ausschluss:
  - Geben Sie eine bestimmte URL ein, z. B. `www.example.com/example.html`
  - Mit Platzhaltern können Sie Web-Adressenmuster definieren:
    - Ein Sternchen (*) ersetzt null oder mehr Zeichen.
    - Ein Fragezeichen (?) ersetzt genau ein Zeichen. Sie können mehrere Fragezeichen benutzen, um eine beliebige Kombination einer bestimmten Anzahl von Zeichen zu ersetzen. So steht ??? z. B. für eine beliebige Folge von genau drei Zeichen.

    In der folgenden Tabelle finden Sie eine Reihe von Beispielsyntaxen für die Angabe von Internet-Adressen.

Syntax	Anwendungsbereich des Ausschlusses
`www.beispiel*`	Jeder Website oder Web-Seite, die mit `www.beispiel` beginnt (unabhängig von der Domänenerweiterung). Der Ausschluss gilt nicht für die Unterdomänen der angegebenen Website, so zum Beispiel `unterdomäne.beispiel.com`.
`*beispiel.com`	Jede Website, die mit `beispiel.com` aufhört, einschließlich aller Seiten und Unterdomänen.
`*Zeichenfolge*`	Jeder Website oder Web-Seite, in deren Adresse die angegebene Zeichenfolge enthalten ist.
`*.com`	Jede Website mit der Domänenerweiterung `.com`, einschließlich aller Seiten und Unterdomänen. Mit dieser Syntax können Sie eine gesamte Top-Level-Domain vom Scan ausschließen.
`www.beispiel?.com`	Jede Internet-Adresse, die mit `www.beispiel?.com` beginnt. Das Fragezeichen kann dabei für jedes beliebige einzelne Zeichen stehen. Beispiele hierfür sind

Syntax	Anwendungsbereich des Ausschlusses
	`www.beispiel1.com` oder `www.beispielA.com`.

- **Anwendung**. Schließt den angegebenen Prozess oder die Anwendung vom Scan aus. So definieren Sie einen Anwendungs-Scan-Ausschluss:
  - Geben Sie den vollständigen Anwendungspfad ein. Zum Beispiel `C:\Programme\Internet Explorer\iexplore.exe`
  - Sie können auch Umgebungsvariablen verwenden, um den Anwendungspfad anzugeben. Zum Beispiel: `%programme%\Internet Explorer\iexplore.exe`
  - Oder Sie verwenden Platzhalter, um alle Anwendungen zusammenzufassen, die einem bestimmten Muster folgen. Zum Beispiel:
    - `c*.exe` erfasst alle Anwendungen, die mit "c" beginnen (z. B. chrome.exe).
    - `??????.exe` umfasst alle Anwendungen, deren Name genau sechs Zeichen lang ist (chrome.exe, safari.exe, usw.).
    - `[^c]*.exe` umfasst alle Anwendungen, außer denen, die mit "c" beginnen.
    - `[^ci]*.exe` umfasst alle Anwendungenimmer außer denen, die mit "c" oder "i" beginnen.

3. Klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** auf der rechten Seite der Tabelle.

Um eine Entität aus der Liste zu löschen, klicken Sie auf die entsprechende ⊗ **Löschen**-Schaltfläche.

Web

In diesem Bereich können Sie die Surf-Sicherheitseinstellungen konfigurieren.

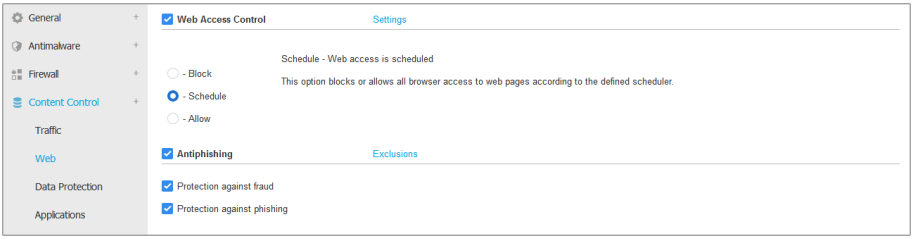
Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- Internet-Zugangssteuerung
- Phishing-Schutz

Internet-Zugangssteuerung

Mit der Internet-Zugangssteuerung können Sie den Internet-Zugang für Benutzer oder Anwendungen für bestimmte Zeiträume zulassen oder blockieren.

Die Webseiten die von der Internet-Zugangssteuerung blockiert werden, werden nicht im Browser angezeigt. Stattdessen wird eine Standardseite angezeigt, die den Nutzer darüber informiert, dass die angeforderte Webseite von der Internet-Zugangssteuerung blockiert wurde.



Richtlinien - Inhaltssteuerung - Web

Mit dem Schalter können Sie die **Internet-Zugangssteuerung** ein- und ausschalten.

Sie haben drei Konfigurationsoptionen:

- Mit **Zulassen** lassen Sie den Internetzugriff immer zu.
- Mit **Blockieren** lassen Sie den Internetzugriff nie zu.
- Mit **Planen** können Sie einen Zeitplan für den Internetzugriff festlegen.

Wenn Sie den Internetzugriff zulassen oder blockieren, können Sie Ausnahmen zu diesen Einstellungen definieren; für ganze Internetkategorien oder für bestimmte einzelne Internetadressen. Klicken Sie auf **Einstellungen** und konfigurieren Sie den Zeitplan bzw. die Ausnahmen wie folgt:

Planer

So schränken Sie den Internet-Zugang auf bestimmte Tageszeiten während der Woche ein:

1. Wählen Sie im Raster die Zeitintervalle, in denen der Internetzugriff blockiert werden soll.

   Sie können auf individuelle Zellen klicken oder eine Zelle anklicken und mit der Maus einen längeren Zeitraum definieren. Wenn Sie erneut auf die Zelle klicken, kehren Sie die Auswahl um.

   Eine neue Auswahl starten Sie, indem Sie, je nach Wunsch, auf **Alle zulassen** oder **Alle blockieren** klicken.

2. Klicken Sie auf **Speichern**.

Beachten Sie
Der Bitdefender-Sicherheitsagent führt unabhängig davon, ob der Internetzugang gesperrt ist, stündlich Updates durch.

Kategorien

Internetkategorienfilter filtern den Zugriff auf Websites dynamisch anhand derer Inhalte. Sie können den Internetkategorienfilter verwenden, um Ausnahmen zur gewählten Aktion (Zulassen oder Blockieren) für ganze Kategorien (z. B. Spiele, nicht jugendfreies Material oder Online-Netzwerke) zu definieren.

So konfigurieren Sie die Internetkategorienfilter:

1. Aktivieren Sie **Internet-Kategorienfilter**.
2. Für eine schnelle Konfiguration können Sie auf eines der vordefinierten Profile (**aggressiv**, **normal**, **tolerant**) klicken. Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala. Wenn Sie den Bereich **Internet-Regeln** unten erweitern, können Sie die vordefinierten Aktionen für bestehende Internetkategorien anzeigen.
3. Wenn Sie mit den Standardeinstellungen nicht zufrieden sein sollten, können Sie einen benutzerdefinierten Filter anlegen:
   a. Wählen Sie **Benutzerdefiniert**.
   b. Klicken Sie auf **Internet-Regeln**, um den entsprechenden Bereich zu erweitern.
   c. Suchen Sie die gewünschte Kategorie in der Liste und wählen Sie die gewünschte Aktion aus dem Menü.
4. Sie können auch **Internetkategorien als Ausnahmen für den Internetzugriff behandeln**, wenn Sie die bestehenden Internetzugriffseinstellungen ignorieren und nur der Internetkategorienfilter benutzen möchten.
5. Klicken Sie auf **Speichern**.

Beachten Sie

- Bestimmte Internetadressen, für die die Berechtigung **Zulassen** eingestellt ist, werden während der Zeiten, zu denen der Internetzugang durch die Internet-Zugangssteuerung blockiert ist, berücksichtigt.
- Das **Zulassen** funktioniert nur, wenn der Internet-Zugang durch die Internet-Zugangssteuerung blockiert ist. Das **Blockieren** funktioniert nur,

wenn der Internet-Zugang über die Internet-Zugangssteuerung zugelassen ist.

- Sie können die Kategorieberechtigung für einzelne Internetadressen außer Kraft setzen, indem Sie sie mit der gegenteiligen Berechtigungen im folgenden Bereich hinzufügen: **Internet-Zugangssteuerung > Einstellungen > Ausschlüsse**. Wenn eine Internetadresse durch die Internet-Kategorienfilter blockiert wird, können Sie für diese Adresse eine Web-Steuerung festlegen und die Berechtigung **Zulassen** erteilen.

Ausschlüsse

Sie können auch Internetregeln erstellen, um bestimmte Internet-Adressen konkret zu blockieren oder zuzulassen. Diese Regeln ignorieren die Einstellungen der Internet-Zugangssteuerung. Wenn also zum Beispiel der Internetzugang durch die Internet-Zugangssteuerung blockiert ist, können Benutzer trotzdem auf bestimmte Webseiten zugreifen.

So legen Sie eine Internetregel an:

1. Aktivieren Sie die Option **Ausschlüsse verwenden**.
2. Geben Sie die Adresse, die Sie zulassen oder blockieren möchten in das Feld **Internetadresse** ein.
3. Wählen Sie **Zulassen** oder **Blockieren** aus dem Menü **Berechtigung**.
4. Klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** auf der rechten Seite der Tabelle, um die Adresse der Liste der Ausnahmen hinzuzufügen.
5. Klicken Sie auf **Speichern**.

So bearbeiten Sie eine Internet-Regel:

1. Klicken Sie auf die Internet-Adresse, die Sie bearbeiten wollen:
2. Die bestehende URL verändern.
3. Klicken Sie auf **Speichern**.

Um eine Internetregel zu entfernen, klicken Sie auf die entsprechende ⊗ **Löschen**-Schaltfläche.

Phishing-Schutz

Der Phishing-Schutz blockiert automatisch bekannte Phishing-Seiten, um zu verhindern, dass Benutzer unbeabsichtigt persönliche oder vertrauliche Informationen an Online-Betrüger weitergeben. Anstelle der Phishing-Seite wird

eine spezielle Warnseite im Browser eingeblendet, die den Benutzer darüber informiert, dass die angeforderte Webseite gefährlich ist.

Wählen Sie **Phishing-Schutz**, um den Phishing-Schutz zu aktivieren. Sie können den Phishing-Schutz über die folgenden Einstellungen an Ihre Bedürfnisse anpassen:

- **Schutz vor Betrug**. Wählen Sie diese Option, wenn Sie den Schutz auf weitere Betrugsarten neben Phishing ausweiten möchten. So zum Beispiel Webseiten von Scheinfirmen, die zwar nicht direkt private Informationen anfordern, aber versuchen, sich als legitime Unternehmen auszugeben und Geld verdienen, indem Sie Menschen so manipulieren, dass Sie eine Geschäftsbeziehung mit ihnen aufnehmen.
- **Schutz vor Phishing-Attacken**. Lassen Sie diese Option aktiviert, um Benutzer vor Phishing-Versuchen zu schützen.

Wenn eine legitime Webseite fälschlicherweise als Phishing-Seite identifiziert und blockiert wird, können Sie diese zur Whitelist hinzufügen, damit Benutzer darauf zugreifen können. Diese Liste sollte nur Websites enthalten, denen Sie uneingeschränkt vertrauen.

So verwalten Sie Phishing-Schutz-Ausnahmen:

1. Klicken Sie auf **Ausschlüsse**.
2. Geben Sie die Internet-Adresse ein und klicken Sie auf die Schaltfläche ⊕ **Hinzufügen**.

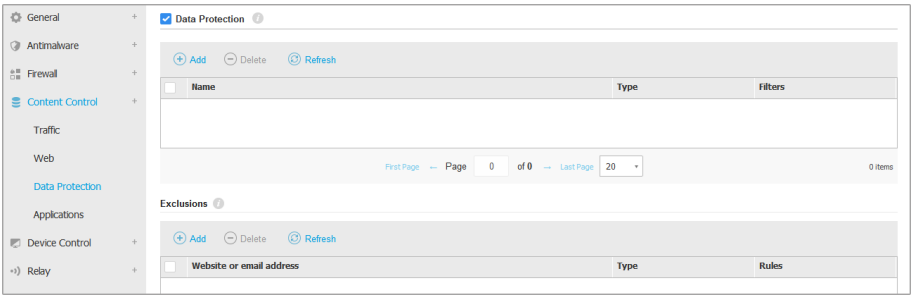
   Wenn Sie eine ganze Website ausschließen möchten, geben Sie den Domainnamen, z. B. `http://www.website.com`, ein; wenn Sie nur eine bestimmte Webseite ausschließen möchten, geben Sie die genaue Internetadresse dieser Seite ein.

   Beachten Sie
   Platzhalter in URLs sind nicht erlaubt.

3. Um eine Ausnahme aus der Liste zu löschen, klicken Sie auf die entsprechende ⊗ **Löschen**-Schaltfläche.
4. Klicken Sie auf **Speichern**.

Datenschutz

Mit dem Identitätsschutz kann der Administrator Regeln definieren, die eine unautorisierte Weitergabe von sensiblen Daten verhindern.



Richtlinien - Inhaltssteuerung - Identitätsschutz

Sie können Regeln erstellen, um personenbezogene oder vertrauliche Daten jeder Art zu schützen, so zum Beispiel:

- Persönliche Kundeninformationen
- Namen und Schlüsseldaten von Entwicklungsprodukten und -technologien
- Kontaktinformationen von Führungskräften im Unternehmen

Geschützte Informationen können Namen, Telefonnummern, Kreditkarten- und Bankdaten, E-Mail-Adressen usw. sein.

Basierend auf den von Ihnen erstellten Identitätsschutzregeln scannt Bitdefender Endpoint Security Tools den Web- und ausgehenden E-Mail-Verkehr nach bestimmten Zeichenfolgen (z. B. Kreditkartennummern). Wird eine Übereinstimmung gefunden, wird die entsprechende Webseite oder E-Mail-Nachricht blockiert, um zu verhindern, dass geschützte Daten versendet werden. Der Benutzer wird sofort über eine Benachrichtigungsseite im Browser oder eine E-Mail über die von Bitdefender Endpoint Security Tools durchgeführte informiert.

So konfigurieren Sie den Identitätsschutz:

1. Markieren Sie das Kästchen, um den Identitätsschutz einzuschalten.
2. Legen Sie Identitätsschutzregeln für alle sensiblen Daten an, die Sie schützen möchten. Um eine Regel anzulegen:

a. Klicken Sie auf die Schaltfläche ⊕**Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird geöffnet.

b. Geben Sie den Namen ein, unter dem die Regel in der Regeltabelle aufgeführt werden soll. Wählen Sie einen eindeutigen Namen, damit Sie oder andere Administrationen die Regel entsprechend zuordnen können.

c. Bitte wählen Sie die zu sichernden Daten.

d. Geben Sie die Daten ein, die Sie schützen möchten (so zum Beispiel die Telefonnummer einer Führungskraft oder den internen Namen eines neuen Produkts in der Entwicklungsphase). Jede beliebige Kombination von Wörtern, Zahlen oder Zeichenfolgen aus alphanumerischen Zeichen und Sonderzeichen (z.B. @, # oder $) ist möglich.

   Geben Sie mindestens fünf Zeichen ein, um ein versehentliches Blockieren von E-Mail-Nachrichten oder Webseiten zu verhindern.

   Wichtig

   Eingegebene Daten werden verschlüsselt auf geschützten Endpunkten gespeichert, können aber über Ihr Control Center-Konto angezeigt werden. Für noch bessere Sicherheit sollten Sie die Daten, die Sie schützen möchten, nicht vollständig eingeben. In diesem Fall müssen Sie die Option **Ganze Wörter abgl.** deaktivieren.

e. Konfigurieren Sie den Datenverkehrs-Scan nach Ihren Anforderungen.

   - **Web-Datenverkehr (HTTP) scannen** - Scannt den HTTP- (Web-) Datenverkehr und blockiert ausgehende Daten, die den Regeln entsprechen.
   - **E-Mail-Verkehr (SMTP) scannen** - Scannt den SMTP- (E-Mail-) Datenverkehr und blockiert alle ausgehenden E-Mail-Nachrichten, die den Regeln entsprechen.

   Sie können wählen, ob die Regeln nur zutreffen, wenn die Daten der Regeln wörtlich übereinstimmen oder ob die komplette Zeichenfolge übereinstimmen muss.

f. Klicken Sie auf **Speichern**. Die neue Regel wird der Liste hinzugefügt.

3. Konfigurieren Sie Ausschlüsse für die Identitätsschutzregeln, damit Benutzer weiterhin geschützte Daten an autorisierte Webseiten und Empfänger versenden

können. Ausschlüsse können global (auf alle Regeln) oder nur auf bestimmte Regeln angewendet werden. Um einen Ausschluss hinzuzufügen:

a. Klicken Sie auf die Schaltfläche **Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird geöffnet.
b. Geben Sie die Web- oder E-Mail-Adresse ein, an die Benutzer geschützte Daten weitergeben dürfen.
c. Wählen Sie die Art des Ausschlusses (Web- oder E-Mail-Adresse).
d. Wählen Sie aus der Tabelle **Regeln** die Identitätsschutzregel(n), auf die dieser Ausschluss angewendet werden soll.
e. Klicken Sie auf **Speichern**. Die neue Ausschlussregel wird der Liste hinzugefügt.

Beachten Sie
Wird eine E-Mail mit blockierten Inhalten an mehrere Empfänger adressiert, wird die Nachricht an die Empfänger verschickt, für die Ausschlüsse definiert wurden.

Um eine Regel oder einen Ausschluss aus der Liste zu entfernen, klicken Sie auf die entsprechende Schaltfläche **Löschen** auf der rechten Seite der Tabelle.

Anwendungen

In diesem Bereich können Sie die Anwendungssteuerung konfigurieren, mit der Sie den Benutzerzugriff auf Anwendungen auf ihren jeweiligen Computern blockieren oder einschränken zu können. Sie können jede beliebige Anwendung sperren – neben Spiel-, Medien- und Chatprogrammen auch andere Arten von Software.

Richtlinien - Inhaltssteuerung - Anwendungen

Um die Anwendungssteuerung zu konfigurieren:

1. Aktivieren Sie die Option **Anwendungssteuerung**.

2. Legen Sie die Anwendungen fest, auf die Sie den Zugriff beschränken möchten. Um den Zugriff auf eine Anwendung einzuschränken:
   a. Klicken Sie auf die Schaltfläche ⊕**Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird geöffnet.
   b. Sie müssen den Pfad der ausführbaren Anwendungsdatei auf den Ziel-Computern angeben. Dafür gibt es zwei Möglichkeiten:
      - Wählen Sie einen vorgegebenen Pfad aus dem Menü und vervollständigen Sie den Pfad im Bearbeitungsfeld nach Bedarf. So müssen Sie für eine Anwendung, die im Ordner `Programme` installiert ist, den Ordner `%Programme` auswählen und den Pfad vervollständigen, indem Sie einen Backslash (\) und den Namen des Anwendungsordners hinzufügen.
      - Geben Sie den vollständigen Pfad in das Bearbeitungsfeld ein. Es empfiehlt sich, (nach Möglichkeit) Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist.
   c. **Zugriffsplaner**. Legen Sie den Anwendungszugriff für bestimmte Tageszeiten während der Woche fest:
      - Wählen Sie im Raster die Zeitintervalle, in denen der Zugriff auf die Anwendung blockiert werden soll. Sie können auf individuelle Zellen klicken oder eine Zelle anklicken und mit der Maus einen längeren Zeitraum definieren. Wenn Sie erneut auf die Zelle klicken, kehren Sie die Auswahl um.
      - Eine neue Auswahl starten Sie, indem Sie, je nach Wunsch, auf **Alle zulassen** oder **Alle blockieren** klicken.
      - Klicken Sie auf **Speichern**. Die neue Regel wird der Liste hinzugefügt.

Um eine Regel aus der Liste zu entfernen, wählen Sie sie aus und klicken Sie auf die Schaltfläche ⊗ **Löschen** am oberen Rand der Tabelle. Wenn Sie eine bestehende Regel bearbeiten möchten, klicken Sie auf die Regel, um das Konfigurationsfenster zu öffnen.

5.2.5. Gerätesteuerung

Mit dem Modul Gerätesteuerung kann mithilfe von in Richtlinien festgelegten Blockier-Regeln und Ausschlüssen verhindert werden, dass sensible Daten unbefugt weitergegeben werden und Infektionen über externe Datenträger ins Netzwerk gelangen. Dies ist für eine große Bandbreite an Gerätearten möglich.

Wichtig
Das Modul Gerätesteuerung steht nur für unterstützte Windows-Betriebssysteme (Arbeitsplatzrechner und Server), nicht aber für Linux oder Mac, zur Verfügung.

Um das Modul Gerätesteuerung nutzen zu können, müssen Sie es zunächst im auf den gewünschten Endpunkten installierten Sicherheitsagenten integrieren und anschließend die Option **Gerätesteuerung** in der Richtlinie, die diesen Endpunkten zugewiesen ist, aktivieren. Ab dann wird der Sicherheitsagent jedes Mal, wenn ein Gerät an einen verwalteten Endpunkt angeschlossen wird, Informationen über dieses Ereignis an das Control Center senden. Die gesendeten Informationen enthalten den Namen des Geräts, die Klasse, die ID und den Zeitpunkt, zu dem das Gerät angeschlossen wurde.

Mit der Gerätesteuerung können Sie Berechtigungen für die folgenden Arten von Geräten verwalten:

- Bluetooth-Geräte
- CDROM-Geräte
- Diskettenlaufwerke
- IEEE 1284.4
- IEEE 1394
- Bildverarbeitungsgeräte
- Modems
- Bandlaufwerke
- Windows für Mobilgeräte
- COM/LPT-Ports
- SCSI Raid
- Drucker
- Netzwerkadapter
- WLAN-Netzwerkkarten
- Interne und externe Speichermedien

Mit der Gerätesteuerung können Sie Berechtigungen von Geräten auf zwei Arten verwalten:

- Berechtigungsregeln definieren
- Berechtigungsausschlüsse definieren

Regeln

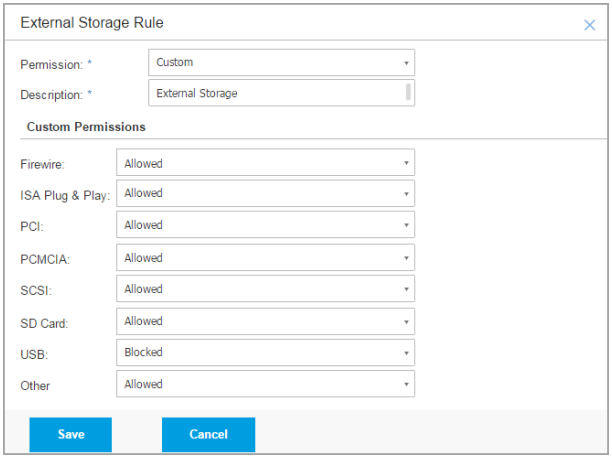
Im Bereich **Regeln** können die Berechtigungen für die mit den Zielendpunkten verbundenen Geräte definiert werden.

So legen Sie die Berechtigungen für einen bestimmten Gerätetyp fest:

1. Gehen Sie zu **Gerätesteuerung > Regeln**.

2. Klicken Sie in der Tabelle auf den Gerätenamen.
3. Wählen Sie einen Berechtigungstyp aus den verfügbaren Optionen. Die verfügbaren Berechtigungen hängen dabei vom Gerätetyp ab:
   - **Zugelassen**: Das Gerät kann auf dem Endpunkt verwendet werden.
   - **Blockiert**: Das Gerät kann nicht auf dem Endpunkt verwendet werden. In diesem Fall gibt der Sicherheitsagent jedes Mal, wenn das Gerät mit dem Endpunkt verbunden wird, eine Meldung aus, die besagt, dass das Gerät blockiert wurde.
   - **Schreibgeschützt**: Von dem Gerät kann nur gelesen werden.
   - **Benutzerdefiniert**: Für jede Art von Anschluss desselben Gerätes, wie Firewire, ISA Plug & Play, PCI, PCMCIA, USB usw., können unterschiedliche Berechtigungen definiert werden. In diesem Fall wird die Liste der für das ausgewählte Gerät verfügbaren Komponenten angezeigt, und Sie können für jede Komponente eine eigene Berechtigung festlegen.

     Für externe Speichermedien können Sie zum Beispiel nur USB blockieren und alle anderen Anschlussarten zulassen.



Richtlinien – Gerätesteuerung – Regeln

Ausschlüsse

Nachdem Sie die Berechtigungsregeln für verschiedene Gerätetypen festgelegt haben, möchten Sie eventuell bestimmte Geräte oder Produktarten von diesen Regeln ausschließen.

Geräteausschlüsse können Sie auf eine von zwei Arten definieren:

- Nach Geräte-ID (oder Hardware-ID); so können konkrete Einzelgeräte ausgeschlossen werden.
- Nach Produkt-ID (oder PID); so können Geräteserien desselben Herstellers ausgeschlossen werden.

So definieren Sie Geräteregelausschlüsse:

1. Gehen Sie zu **Gerätesteuerung > Ausschlüsse**.
2. Aktivieren Sie die Option **Ausschlüsse**.
3. Klicken Sie auf die Schaltfläche **Hinzufügen** am oberen Ende der Tabelle.
4. Wählen Sie, auf welche Art Sie Ausschlüsse hinzufügen möchten:
   - **Manuell**. Mit dieser Methode müssen Sie jede einzelne Geräte-ID oder Produkt-ID, die Sie ausschließen möchten, zur Hand haben und einzeln eingeben:
     a. Wählen Sie den Ausschlusstyp (nach Produkt-ID oder nach Geräte-ID).
     b. Geben Sie im Feld **Ausnahmen** die IDs ein, die Sie ausschließen möchten:
     c. Geben Sie im Feld **Beschreibung** einen aussagekräftigen Namen ein, anhand dessen Sie das Gerät oder die Geräteserie wiedererkennen können.
     d. Wählen Sie den Berechtigungstyp für die entsprechenden Geräte (Zugelassen oder Blockiert).
     e. Klicken Sie auf **Speichern**.
   - **Von gefundenen Geräten**. Mit dieser Methode können Sie die Geräte-IDs oder Produkt-IDs, die Sie ausschließen möchten, aus einer Liste aller in Ihrem Netzwerk gefundenen Geräte auswählen (nur verwaltete Endpunkte):
     a. Wählen Sie den Ausschlusstyp (nach Produkt-ID oder nach Geräte-ID).
     b. Wählen Sie aus der Tabelle **Ausschlüsse** die IDs, die Sie ausschließen möchten:
        – Bei Ausschluss nach Geräte-ID müssen Sie jedes einzelne Gerät in der Liste auswählen, das Sie ausschließen möchten.

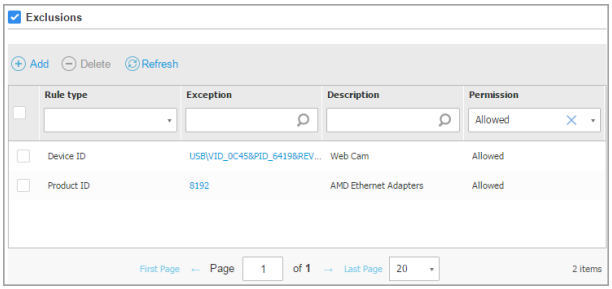
- Bei Ausschluss nach Produkt-ID können Sie ein Gerät auswählen und damit alle Geräte mit dieser Produkt-ID ausschließen.

c. Geben Sie im Feld **Beschreibung** einen aussagekräftigen Namen ein, anhand dessen Sie das Gerät oder die Geräteserie wiedererkennen können.
d. Wählen Sie den Berechtigungstyp für die entsprechenden Geräte (Zugelassen oder Blockiert).
e. Klicken Sie auf **Speichern**.

Wichtig
Geräte, die bei der Installation von Bitdefender Endpoint Security Tools bereits mit den Endpunkten verbunden waren, werden erst nach einem Neustart der entsprechenden Endpunkte gefunden.

Alle Geräteausschlüsse werden in der Tabelle **Ausschlüsse** aufgeführt.

So entfernen Sie einen Ausschluss:
a. Markieren Sie den Ausschluss in der Tabelle.
b. Klicken Sie auf die Schaltfläche ⊕ **Löschen** am oberen Rand der Tabelle.



Richtlinien - Gerätesteuerung - Ausschlüsse

5.2.6. Relais

In diesem Bereich können Sie Kommunikations- und Update-Einstellungen für Endpunkte mit Relais-Rolle definieren.

Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- Kommunikation
- Update

Kommunikation

Im Reiter **Kommunikation** finden Sie Proxy-Einstellungen für die Kommunikation zwischen Relais-Endpunkten und den GravityZone-Komponenten.

Bei Bedarf können Sie die Kommunikation zwischen einzelnen Relais-Endpunkten und Bitdefender Cloud Services/GravityZone Control Center mit den folgenden Einstellungen einzeln konfigurieren:

- **Installationseinstellungen behalten**, wenn dieselben Proxy-Einstellungen verwendet werden sollen, die im Installationspaket definiert sind.
- **Den im Bereich Allgemein definierten Proxy verwenden**, wenn Sie die Proxy-Einstellungen verwenden möchten, die in der aktuellen Richtlinie im Bereich **Allgemein > Einstellungen** definiert sind.
- **Nicht verwenden**, wenn die Zielendpunkte nicht über einen Proxy mit den Bitdefender-Komponenten kommunizieren.

Update

In diesem Bereich können Sie die Update-Einstellungen für Endpunkte mit Relais-Rolle definieren:

- Im Bereich **Update** können Sie die folgenden Einstellungen konfigurieren:
  - Der zeitliche Abstand, in dem die Relais-Endpunkte nach Updates suchen.
  - Der Ordner auf dem Relais-Endpunkt, in dem die Produkt- und Signatur-Updates gespeichert und gespiegelt werden. Wenn Sie einen bestimmten Download-Ordner festlegen möchten, geben Sie einfach den vollständigen Pfad in das entsprechende Feld ein.

    Wichtig
    Es empfiehlt sich, einen Ordner festzulegen, der nur für Produkt- und Signatur-Updates da ist. Ein Ordner, in dem auch Systemdateien oder private Dateien liegen, sollte nicht gewählt werden.

- **Benutzerdefinierte Update-Server festlegen**. Der Standard-Update-Server für Relais-Agenten ist: http://upgrade.bitdefender.com. Sie können einen anderen Update-Server festlegen, indem Sie die IP-Adresse oder den lokalen Hostnamen einer oder mehrerer Relais-Maschinen in Ihrem Netzwerk eingeben und dann deren Priorität mithilfe der Pfeile festlegen, die angezeigt werden, wenn Sie mit

dem Mauszeiger auf den jeweiligen Server gehen. Wenn der erste Update-Server in der Liste nicht verfügbar ist, wird der zweite verwendet usw.

So definieren Sie einen benutzerdefinierten Update-Server:

1. Aktivieren Sie die Option **Benutzerdefinierte Update-Server festlegen**.
2. Geben Sie die Adresse des neuen Update-Servers in das Feld **Ziel hinzufügen** ein. Verwenden Sie dazu eine der folgenden Syntaxoptionen:
   - `update_server_ip:port`
   - `update_server_name:port`

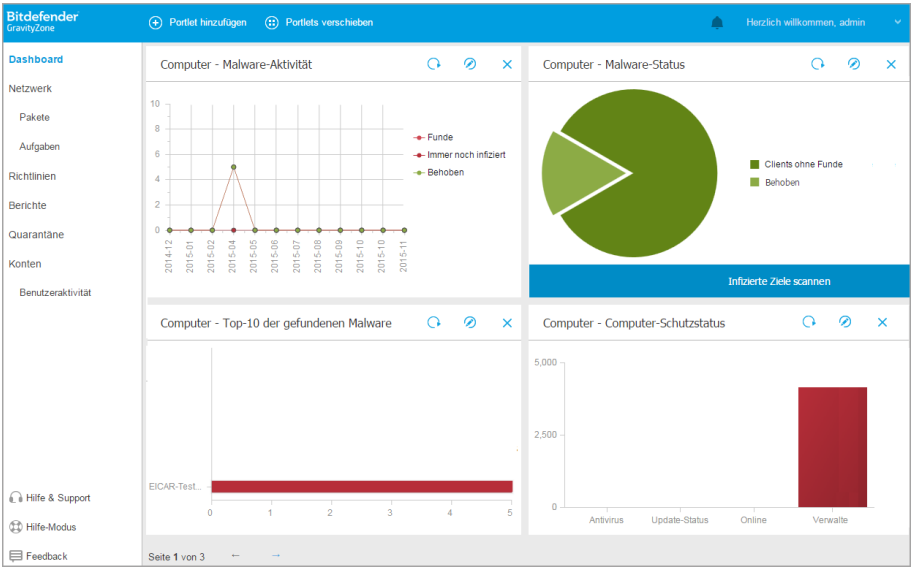
   Der Standard-Port ist 7074.
3. Falls der Relais-Endpunkt über einen Proxy-Server mit dem lokalen Update-Server kommuniziert, aktivieren Sie **Proxy benutzen**. Die Proxy-Einstellungen, die im Bereich **Allgemein > Einstellungen** definiert sind, werden berücksichtigt.
4. Klicken Sie auf die Schaltfläche ⊕ **Hinzufügen** auf der rechten Seite der Tabelle.
5. Legen Sie mithilfe der Pfeile ⌃ und ⌄ in der Spalte **Aktion** die Priorität der definierten Udpate-Server fest. Wenn der erste Update-Server in der Liste nicht verfügbar ist, wird der zweite verwendet usw.

Um einen Pfad aus der Liste zu löschen, klicken Sie auf die entsprechende ⊗ **Löschen**-Schaltfläche. Es ist zwar möglich, die standardmäßige Update-Adresse zu entfernen, dies wird jedoch nicht empfohlen.

6. ÜBERWACHUNGS-DASHBOARD

Das Control Center-Dashboard ist eine individuell anpassbare Oberfläche, die Ihnen einen schnellen Überblick über die Sicherheitslage der geschützten Endpunkte verschafft.

In den Dashboard-Portlets werden verschiedenste Echtzeit-Sicherheitsinformationen in übersichtlichen Diagrammen angezeigt. Sie bieten einen schnellen Überblick über Bereiche, die Ihre Aufmerksamkeit erfordern.



Das Dashboard

Was Sie über Dashboard-Portlets wissen sollten:

- Die Control Center verfügt über verschiedene vordefinierte Dashboard-Portlets.
- Jedes Dashboard-Portlet enthält im Hintergrund einen detaillierten Bericht, der mit einem einfachen Klick auf das Diagramm abgerufen werden kann.
- Es gibt eine Reihe verschiedener Portlet-Typen, die unterschiedliche Informationen über den Schutz Ihrer Endpunkte enthalten, so zum Beispiel Update-Status, Malware-Status, Firewall-Aktivität usw. Weitere Informationen

zu den verschiedenen Arten von Dashboard-Portlets finden Sie unter „Verfügbare Berichtstypen“ (S. 140).

- Die in den Portlets angezeigten Informationen beziehen sich nur auf Endpunkte unter Ihrem Konto. Sie können die Ziele und Präferenzen jedes Portlets mit dem Befehl **Portlet bearbeiten** an Ihre Bedürfnisse anpassen.
- Klicken Sie auf die einzelnen Einträge in der Diagrammlegende, um die entsprechende Variable, falls verfügbar, auf dem Graphen anzuzeigen bzw. auszublenden.
- Die Portlets werden in Vierergruppen angezeigt. Verwenden Sie die Pfeile unten auf der Seite, um zwischen den Portlet-Gruppen hin und her zu schalten.
- Bei verschiedenen Berichttypen haben Sie die Möglichkeit, sofort bestimmte Aufgaben auf den Zielendpunkten ausführen zu lassen, ohne dazu erst auf die Seite **Netzwerk** wechseln zu müssen; so können Sie z. B. infizierte Endpunkte scannen oder Endpunkte aktualisieren. Über die Schaltfläche am unteren Rand des Portlets können Sie die entsprechende Aktion ausführen.

Das Dashboard lässt sich nach individuellen Vorlieben leicht konfigurieren. Sie können Portlet-Einstellungen bearbeiten, neue Portlets hinzufügen, Portlets entfernen oder die bestehenden Portlets neu anordnen.

6.1. Portlet-Daten neu laden

Um sicherzustellen, dass das Portlet die aktuellsten Informationen anzeigt, klicken Sie auf das **Neu laden**-Symbol in der entsprechenden Titelleiste.

6.2. Portlet-Einstellungen bearbeiten

Einige der Portlets enthalten Statusinformationen, andere zeigen die Sicherheitsereignisse im letzten Berichtszeitraum an. Sie können den Berichtszeitraum eines Portlets anzeigen und konfigurieren, indem Sie auf die das Symbol **Portlet bearbeiten** in der entsprechenden Titelleiste klicken.

6.3. Ein neues Portlet hinzufügen

Sie können andere Portlets hinzufügen, um bestimmte Informationen angezeigt zu bekommen.

So fügen Sie ein neues Portlet hinzu:

1. Gehen Sie zur Seite **Dashboard**.

2. Klicken Sie auf die Schaltfläche **Portlet hinzufügen** am oberen Rand der Konsole. Das Konfigurationsfenster wird geöffnet.
3. Im Reiter **Details** können Sie die Details des Portlets konfigurieren:
   - Art des Hintergrundberichts
   - Aussagekräftiger Portlet-Name
   - Das Intervall, in dem die Ereignisse berichtet werden

   Weitere Informationen zu verfügbaren Berichtstypen finden Sie unter „Verfügbare Berichtstypen“ (S. 140).
4. Wählen Sie im Reiter **Ziele** die Netzwerkobjekte und Gruppen, die Sie einbeziehen möchten.
5. Klicken Sie auf **Speichern**.

6.4. Ein Portlet entfernen

Sie können ein Portlet ganz einfach entfernen, indem Sie in seiner Titelleiste auf das Symbol **Entfernen** klicken. Wenn Sie ein Portlet einmal entfernt haben, können Sie es nicht wiederherstellen. Sie können aber ein neues Portlet mit genau denselben Einstellungen erstellen.

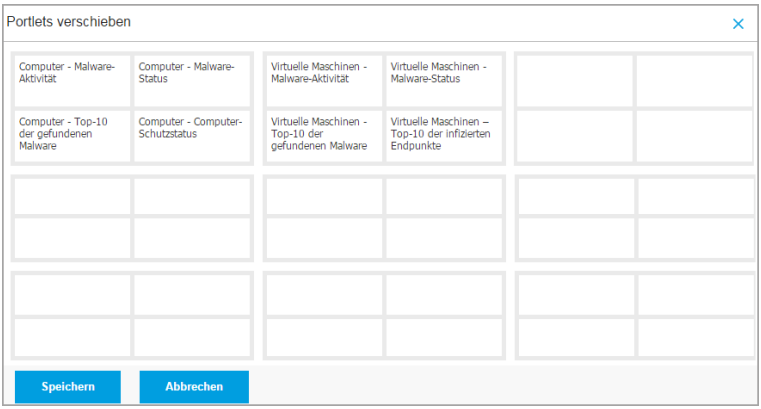
6.5. Portlets neu anordnen

Sie können die Portlets im Dashboard ganz nach Ihren Bedürfnissen anordnen. So ordnen Sie die Portlets neu an:

1. Gehen Sie zur Seite **Dashboard**.
2. Klicken Sie auf die Schaltfläche **Portlets verschieben** am oberen Rand der Konsole. Die Portlet-Übersicht wird angezeigt.
3. Ziehen Sie die einzelnen Portlets mit der Maus an die gewünschte Stelle. Alle anderen Portlets zwischen der alten und der neuen Position behalten ihre Anordnung bei.

   Beachten Sie
   Sie können Portlets nur innerhalb der bestehenden Positionen verschieben.

4. Klicken Sie auf **Speichern**.



Das Fenster "Portlets verschieben"

7. BERICHTE VERWENDEN

Mit Control Center können Sie Berichte über den Sicherheitsstatus der verwalteten Netzwerkobjekte zentral erstellen und anzeigen. Die Berichte können zu verschiedenen Zwecken eingesetzt werden, wie zum Beispiel:

- Einhaltung der Unternehmenssicherheitsrichtlinien überwachen und sicherstellen.
- Überprüfung und Bewertung des Netzwerksicherheitsstatus.
- Sicherheitsprobleme, Bedrohungen und Sicherheitslücken im Netzwerk erkennen.
- Sicherheitsvorfälle und Malware-Aktivität überwachen.
- Bereitstellung von übersichtlichen Daten zur Netzwerksicherheit für die Unternehmensführung.

Es stehen verschiedene Berichtstypen zur Verfügung, damit Sie einfachen Zugriff auf die von Ihnen benötigten Informationen erhalten. Diese Informationen werden in übersichtlichen interaktiven Diagrammen und Grafiken dargestellt, so dass Sie schnell den Sicherheitsstatus des Netzwerkes überprüfen und eventuelle Sicherheitsprobleme erkennen können.

Die Berichte können Daten vom gesamten Netzwerk der verwalteten Netzwerkobjekte beinhalten oder sich auf ausgewählte Gruppen konzentrieren. So können Sie mit einem einzigen Bericht folgendes erfahren:

- Statistische Daten zu allen oder Gruppen von verwalteten Netzwerkobjekten.
- Detailinformationen für jedes verwaltete Netzwerkobjekt.
- Die Liste von Computern, die bestimmte Kriterien erfüllen (zum Beispiel solche, deren Malware-Schutz deaktiviert ist).

Einige Berichte ermöglichen es Ihnen auch, die in Ihrem Netzwerk gefundenen Probleme schnell und unkompliziert zu beheben. So können Sie z. B. direkt aus dem Bericht heraus alle gewünschten Netzwerkobjekte aktualisieren, ohne eine Aktualisierungsaufgabe von der Seite **Netzwerk** ausführen zu müssen.

Alle geplanten Berichte stehen im Control Center zur Verfügung, Sie können sie aber auch auf Ihrem Computer speichern oder per E-Mail versenden.

Verfügbare Formate sind u.a. Portable Document Format (PDF) und Comma-Separated Values (CSV).

7.1. Verfügbare Berichtstypen

Im Folgenden werden die verschiedenen Berichttypen für physische und virtuelle Maschinen beschrieben:

Phishing-Schutz-Aktivität

Informiert Sie über die Aktivität des Phishing-Schutz-Moduls von Bitdefender Endpoint Security Tools. Hier sehen Sie die Anzahl der blockierten Phishing-Websites auf den ausgewählten Endpunkten. Sie können auf die Links in der Spalte **Blockierte Websites** klicken, um die URLs der Websites anzuzeigen, wie oft und wann sie zuletzt blockiert wurden.

Blockierte Anwendungen

Informiert Sie über die Aktivität des Anwendungssteuerungsmoduls von Bitdefender Endpoint Security Tools. Hier sehen Sie die Anzahl der blockierten Anwendungen auf den ausgewählten Endpunkten. Wenn Sie auf die entsprechende Zahl klicken, können Sie für jedes Ziel zusätzliche Informationen zu den blockierten Anwendungen, die Anzahl der ausgelösten Ereignisse und den Zeitpunkt des zuletzt blockierten Ereignisses anzeigen.

Vom Verhaltens-Scan blockierte Anwendungen

Informiert Sie über die von der Active Virus Control (AVC) / dem Angrifferkennungssystem (IDS) blockierte Anwendungen. Sie können die Anzahl der von AVC/IDS blockierten Anwendungen für jeden ausgewählten Endpunkt anzeigen. Klicken Sie auf die Anzahl der blockierten Anwendungen für den gewünschten Endpunkt, um die Liste der blockierten Anwendungen und die dazugehörigen Informationen anzuzeigen (Anwendungsname, Grund für die Blockierung, Anzahl der blockierten Versuche sowie Datum und Zeitpunkt des zuletzt blockierten Versuchs).

Blockierte Webseiten

Informiert Sie über die Aktivität des Moduls Internet-Zugangssteuerung von Bitdefender Endpoint Security Tools. Für jedes Ziel können Sie die Anzahl der blockierten Websites sehen. Wenn Sie auf eine dieser Zahlen klicken, können Sie zusätzliche Informationen anzeigen:

- URL und Kategorie der Website
- Anzahl der versuchten Aufrufe pro Website
- Datum und Uhrzeit des letzten versuchten Aufrufs.

Datenschutz

Informiert Sie über die Aktivität des Identitätsschutzmoduls von Bitdefender Endpoint Security Tools. Hier sehen Sie die Anzahl der blockierten E-Mails und Websites auf den ausgewählten Endpunkt.

Aktivität der Gerätesteuerung

Informiert Sie über Ereignisse beim Zugriff auf die Endpunkte über überwachte Geräte. Sie können für jeden Zielendpunkt die Anzahl der zugelassenen/blockierten Zugriffs- und Schreibgeschützt-Ereignisse anzeigen. Wenn Ereignisse eingetreten sind, können Sie zusätzliche Informationen dazu anzeigen, indem Sie auf die entsprechenden Zahlen klicken. Angezeigt werden Details zu:

- Auf der Maschine angemeldeter Benutzer
- Gerätetyp und -ID
- Gerätehersteller und Produkt-ID
- Datum und Uhrzeit des Ereignisses.

Status der Endpunktmodule

Gibt einen Überblick über den Status der Sicherheitsmodule von Bitdefender Endpoint Security Tools für die ausgewählten Endpunkte. Sie sehen, welche Module aktiv sind und welche deaktiviert oder nicht installiert sind.

Status des Endpunktschutzes

Bietet Ihnen verschiedene Statusinformationen zu ausgewählten Endpunkten in Ihrem Netzwerk.

- Status des Malware-Schutzes
- Update-Status von Bitdefender Endpoint Security Tools
- Status der Netzwerkaktivität (online/offline)
- Verwaltungsstatus

Sie können nach Sicherheitsaspekt und -status filtern, um die Informationen zu erhalten, nach denen Sie suchen.

Firewallaktivität

Informiert Sie über die Aktivität des Firewall-Moduls von Bitdefender Endpoint Security Tools. Hier sehen Sie die Anzahl der blockierten Verbindungsversuche und Port-Scans auf den ausgewählten Endpunkten.

Malware-Aktivität

Zeigt Ihnen übergreifende Informationen zu Malware-Bedrohungen, die über einen festgelegten Zeitraum auf den ausgewählten Endpunkten gefunden wurden. Sie können Folgendes sehen:

- Anzahl der Funde (gefundene Dateien, die mit Malware infiziert sind)
- Anzahl der behobenen Infektionen (Dateien, die erfolgreich desinfiziert oder in die Quarantäne verschoben wurden)
- Anzahl der nicht behobenen Infektionen (Dateien, die nicht desinfiziert werden konnten, auf die der Zugriff aber verweigert wurde; so z. B. eine infizierte Datei, die mit einem proprietären Archivformat gespeichert wurde)

Für jede gefundene Bedrohung können Sie die Liste der betroffenen Endpunkte und Dateipfade anzeigen, indem Sie in den Spalten der Desinfektionsergebnisse auf die entsprechenden Links klicken. Wenn Sie z. B. in der Spalte **Behoben** auf die Zahl klicken, werden die Dateien und Endpunkte angezeigt, von denen die Bedrohung entfernt wurde.

Malware-Status

Hilft Ihnen dabei herauszufinden, wie viele und welche der ausgewählten Endpunkte über einen bestimmten Zeitraum von Malware-Infektionen betroffen waren und wie mit der Bedrohung umgegangen wurde.

Endpunkte werden nach diesen Kriterien in Gruppen aufgeteilt:

- Endpunkte ohne Funde (über den festgelegten Zeitraum wurde keine Malware-Bedrohung gefunden).
- Endpunkte mit behobener Malware (alle als infiziert erkannte Dateien wurden erfolgreich desinfiziert oder in die Quarantäne verschoben)
- Immer noch mit Malware infizierte Endpunkte (der Zugriff auf einige der infizierten Dateien wurde verweigert)

Für jeden Endpunkt können Sie die Liste der Bedrohungen und der betroffenen Dateipfade anzeigen, indem Sie in den Spalten der Desinfektionsergebnisse auf die entsprechenden Links klicken.

Netzwerkstatus

Zeigt Ihnen detaillierte Information zum allgemeinen Sicherheitsstatus der ausgewählten Endpunkte. Endpunkte werden nach diesen Kriterien in Gruppen aufgeteilt:

- Problemstatus

- Verwaltungsstatus
- Infektionsstatus
- Status des Malware-Schutzes
- Produktupdate Status
- Lizenzierungsstatus
- Der Netzwerkaktivitätsstatus jedes Endpunktes (online/offline). Wenn der Endpunkt zum Zeitpunkt der Berichterstellung offline ist, werden Datum und Uhrzeit angezeigt, zu der er zuletzt vom Control Center gesehen wurde.

Top-10 der gefundenen Malware
Zeigt Ihnen die 10 häufigsten Malware-Bedrohungen, die über einen bestimmten Zeitraum auf den ausgewählten Endpunkten gefunden wurden.

> **Beachten Sie**
> In der Detailtabelle werden alle Endpunkte angezeigt, die von einer der Top-10 der gefundenen Malware infiziert wurden.

Top-10 der infizierten Endpunkte
Zeigt von den ausgewählten Endpunkten die 10 mit den meisten Infektionen an, sortiert nach der Anzahl der Funde während eines bestimmten Zeitraums.

> **Beachten Sie**
> In der Detailtabelle wird sämtliche Malware angezeigt, die auf den Top-10 der infizierten Endpunkten gefunden wurde.

Update-Status
Zeigt Ihnen den Update-Status des auf den ausgewählten Zielen installierten Bitdefender Endpoint Security Tools an. Der Update-Status bezieht sich auf die Produktversion und die Version der Engines (Signaturen).

Über die verfügbaren Filter können Sie schnell feststellen, welche Clients in den letzten 24 Stunden aktualisiert und welche nicht aktualisiert wurden.

Upgrade-Status
Zeigt an, welche Sicherheitsagenten auf den ausgewählten Zielen installiert sind und ob es eine neuere Version dazu gibt.

Auf Endpunkten mit alten Sicherheitsagenten können Sie ganz einfach den neuesten unterstützten Sicherheitsagenten installieren, indem Sie auf die Schaltfläche **Upgrade durchführen** klicken.

Beachten Sie
Dieser Bericht steht nur zur Verfügung, wenn ein Upgrade für die GravityZone-Lösung durchgeführt wurde.

7.2. Berichte erstellen

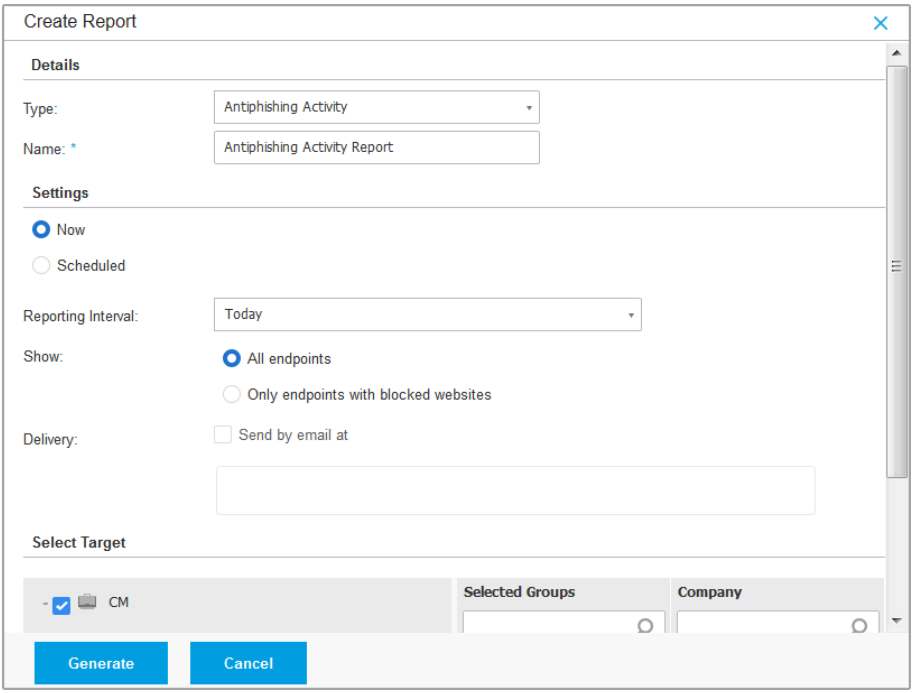
Sie können zwei verschiedene Kategorien von Berichten erstellen:

- **Sofortberichte.** Sofortberichte werden automatisch angezeigt, sobald sie erstellt wurden.
- **Geplante Berichte.** Berichte können so geplant werden, dass sie in regelmäßigen Abständen und/oder zu einem bestimmten Zeitpunkt erstellt werden. Eine Liste aller geplanten Berichte finden Sie auf der Seite **Berichte**.

Wichtig
Sofortberichte werden automatisch gelöscht, wenn Sie die Berichtsseite schließen. Geplante Berichte werden auf der Seite **Berichte** gespeichert und angezeigt.

Um einen Bericht zu erstellen:

1. Gehen Sie zur Seite **Berichte**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen** am oberen Ende der Tabelle. Ein Konfigurationsfenster wird geöffnet.



Berichtsoptionen

3. Wählen Sie den gewünschten Berichtstyp aus dem Menü aus. Weitere Informationen finden Sie unter „Verfügbare Berichtstypen“ (S. 140).
4. Geben Sie einen eindeutigen Namen für den Bericht ein. Wenn Sie einen Namen festlegen, berücksichtigen Sie den Berichtstyp, das Berichtsziel und unter Umständen auch die Berichtsoptionen.
5. Konfigurieren Sie die Wiederholung des Berichts:
   - Mit **Jetzt** erstellen Sie einen Sofortbericht.
   - Mit **Geplant** können Sie den Bericht so konfigurieren, dass er regelmäßig nach einem gewünschten Intervall generiert wird:
     – Stündlich. Immer nach einer festgelegten Anzahl von Stunden.
     – Täglich. Hierbei können Sie auch die Startzeit (Stunde und Minute) festlegen.

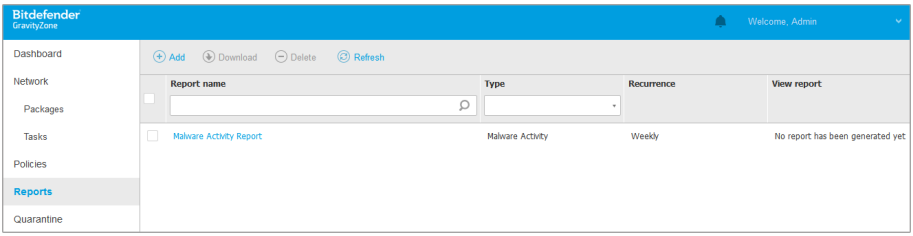
  - Wöchentlich, am festgelegten Wochentag zur festgelegten Startzeit (Stunde und Minute).
  - Monatlich, am festgelegten Tag des Monats zur festgelegten Startzeit (Stunde und Minute).

6. Für die meisten Berichtstypen müssen Sie das Intervall angeben, auf das sich die im Bericht enthaltenen Daten beziehen. Der Bericht zeigt nur Daten aus dem gewählten Zeitraum an.
7. Viele Berichtsarten enthalten Filtermöglichkeiten, damit Sie die für Sie interessanten Informationen schnell finden können. Verwenden Sie die Filtermöglichkeiten im Bereich **Anzeigen**, um nur die gewünschten Informationen abzurufen.

   Für einen **Update-Status**-Bericht können Sie zum Beispiel auf Wunsch nur die Netzwerkobjekte anzeigen, die nicht aktualisiert wurden, oder diejenigen, die neu gestartet werden müssen, um das Update abzuschließen.
8. **Zustellung**. Um einen geplanten Bericht als E-Mail geschickt zu bekommen, markieren Sie das entsprechende Kästchen. Geben Sie die gewünschten E-Mail-Adresse in das Feld darunter ein.
9. **Ziel auswählen**. Scrollen Sie nach unten, das Ziel des Berichts zu konfigurieren. Wählen Sie eine oder mehrere Gruppen von Endpunkten, die Sie in den Bericht einbeziehen möchten.
10. Klicken Sie je nach Wiederholungsintervall auf **Generieren**, um einen Sofortbericht zu erstellen, oder auf **Speichern**, um einen geplanten Bericht zu erstellen.
    - Ein Sofortbericht wird sofort angezeigt, nachdem Sie auf **Generieren** klicken. Die Zeit, die bis zur Fertigstellung eines Berichts benötigt wird, hängt von der Anzahl der verwalteten Netzwerkobjekte ab. Bitte warten Sie, bis der angeforderte Bericht erstellt wurde.
    - Der geplante Bericht wird in der Liste auf der Seite **Berichte** angezeigt. Nachdem eine Berichtsinstanz generiert wurde, können Sie den Bericht anzeigen, indem Sie auf den entsprechenden Link in der Spalte **Bericht anzeigen** auf der Seite **Berichte** klicken.

7.3. Geplante Berichte anzeigen und verwalten

Gehen Sie zum Anzeigen und Verwalten geplanter Berichte zur Seite **Berichte**.



Die Berichteseite

Alle geplanten Berichte werden zusammen mit nützlichen Informationen zu den Berichten in einer Tabelle angezeigt:

- Name und Art des Berichts
- Berichtwiederholung
- Zuletzt generierte Instanz

Beachten Sie
Geplante Berichte sind nur für den Benutzer verfügbar, der diese auch erstellt hat.

Um Berichte nach einer Spalte zu ordnen, klicken Sie einfach auf die Überschrift der jeweiligen Spalte. Mit einem erneuten Klick auf die Spaltenüberschrift können Sie die Sortierungsrichtung ändern

Um die Suche nach Informationen zu beschleunigen, verwenden Sie die Suchfelder oder die Filtermöglichkeiten unter den Spaltenüberschriften.

Sie können das Suchfeld leeren, indem Sie mit dem Mauszeiger darüber fahren und auf das × **Löschen**Symbol klicken.

Um sicherzustellen, dass die neuesten Informationen angezeigt werden, klicken Sie am oberen Rand der Tabelle auf **Neu laden**.

7.3.1. Berichte betrachten

So zeigen Sie einen Bericht an:

1. Gehen Sie zur Seite **Berichte**.
2. Sortieren Sie die Berichte nach Namen, Typ oder Wiederholung, um den gewünschten Bericht leichter zu finden.

3. Klicken Sie in der Spalte **Bericht anschauen** auf den entsprechenden Link, um den Bericht anzuzeigen. Die jüngste Berichtsinstanz wird angezeigt.

   Wie Sie alle Instanzen eines Berichts anzeigen, erfahren Sie unter„Berichte speichern“ (S. 151)

Alle Berichte haben eine Zusammenfassungsteil (die obere Hälfte der Berichtsseite) und einen Detailsteil (die untere Hälfte der Berichtsseite).

- Der Zusammenfassungsbereich enthält statistische Daten (Kuchendiagramme und Grafiken) für alle Netzwerkobjekte sowie allgemeine Informationen über den Bericht wie den Berichtszeitraum (sofern anwendbar), Berichtsziel, usw.
- Der Detailbereich enthält Informationen zu allen entsprechenden Netzwerkobjekten.

Beachten Sie

- Sie können die im Diagramm angezeigten Informationen anpassen, indem Sie auf die Einträge in der Legende klicken und damit die entsprechenden Daten anzeigen oder ausblenden.
- Klicken Sie auf den Bereich der Grafik (Kuchensegment oder Balken), der Sie interessiert, um in der Tabelle Details dazu anzuzeigen.

7.3.2. Geplante Berichte bearbeiten

Beachten Sie

Wenn Sie einen geplanten Bericht bearbeiten, werden sämtliche Änderungen mit der nächsten Ausführung des Berichts wirksam. Zuvor erstellte Berichte sind von den Änderungen nicht betroffen.

Um die Einstellungen eines geplanten Berichts zu ändern:

1. Gehen Sie zur Seite **Berichte**.
2. Klicken Sie auf den Berichtnamen.
3. Ändern Sie die Berichtseinstellungen nach Bedarf. Sie können die folgenden Änderungen vornehmen:
   - **Berichtsname.** Geben Sie dem Bericht einen eindeutigen Namen, der seinen Inhalt widerspiegelt. Wenn Sie einen Namen festlegen, berücksichtigen Sie den Berichtstyp, das Berichtsziel und unter Umständen auch die

Berichtsoptionen. Berichte die anhand eines geplanten Berichts erstellt werden, erhalten auch den entsprechenden Namen.

- **Berichtswiederholung (geplant).** Sie können den Bericht so planen, dass er in regelmäßigen Abständen automatisch wiederholt wird: stündlich (nach einer festgelegten Anzahl von Stunden), täglich (zu einer bestimmten Uhrzeit), wöchentlich (an einem bestimmten Wochentag zu einer bestimmten Uhrzeit) oder monatlich (an einem bestimmten Tag des Monats zu einer bestimmten Uhrzeit). Abhängig von dem ausgewählten Zeitplan wird der Bericht nur Daten vom letzten Tag, aus der letzten Woche oder dem letzten Monat enthalten.
- **Einstellungen**
  - Sie können den Bericht so planen, dass er in regelmäßigen Abständen automatisch wiederholt wird: stündlich (nach einer festgelegten Anzahl von Stunden), täglich (zu einer bestimmten Uhrzeit), wöchentlich (an einem bestimmten Wochentag zu einer bestimmten Uhrzeit) oder monatlich (an einem bestimmten Tag des Monats zu einer bestimmten Uhrzeit). Abhängig von dem ausgewählten Zeitplan wird der Bericht nur Daten vom letzten Tag, aus der letzten Woche oder dem letzten Monat enthalten.
  - Der Bericht wird nur Daten aus dem ausgewählten Intervall enthalten. Sie können das Intervall ab der nächsten Ausführung ändern.
  - Die meisten Berichte enthalten Filtermöglichkeiten, damit Sie die für Sie interessanten Informationen schnell finden können. Wenn Sie den Bericht in der Konsole anzeigen, sind unabhängig von den gewählten Optionen immer alle Informationen verfügbar. Wenn Sie den Bericht herunterladen oder per E-Mail versenden, werden nur die Berichtszusammenfassung und die ausgewählten Informationen in der PDF-Datei enthalten sein. Die Berichtsdetails sind nur im CSV-Format verfügbar.
  - Sie können den Bericht auch per E-Mail erhalten.
- **Ziel wählen.** Die ausgewählte Option weist auf die Art des aktuellen Berichtsziels hin (entweder Gruppen oder einzelne Netzwerkobjekte). Klicken Sie auf den entsprechenden Link, um das aktuelle Berichtsziel anzuzeigen. Sie können das Berichtsziel ändern, indem Sie die Gruppen oder Netzwerkobjekte auswählen, die in dem Bericht eingeschlossen werden sollen.

4. Klicken Sie **Speichern**, um die Änderungen zu speichern.

7.3.3. Geplante Berichte löschen

Wenn ein geplanter Bericht nicht mehr benötigt wird, empfiehlt es sich, diesen zu löschen. Durch das Löschen eines geplanten Berichts werden alle Instanzen, die dieser bis zu diesem Zeitpunkt automatisch erstellt hat, gelöscht.

Um einen geplanten Bericht zu löschen:

1. Gehen Sie zur Seite **Berichte**.
2. Wählen Sie den Bericht, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche ⊖ **Löschen** am oberen Rand der Tabelle.

7.4. Berichtbasierte Aktionen ausführen

Die meisten Berichte stellen nur Probleme in Ihrem Netzwerk dar, manche geben Ihnen jedoch auch einige Optionen an die Hand, um diese Probleme mit ein paar einfachen Klicks zu beheben.

Wenn Sie die im Bericht dargestellten Probleme lösen möchten, können Sie dazu einfach auf auf die entsprechende Schaltfläche in der Symbolleiste über der Tabelle klicken.

Beachten Sie
Sie benötigen **Netzwerk verwalten**-Rechte, um diese Aktionen auszuführen.

Für jeden Bericht stehen die folgenden Optionen zur Verfügung:

Update-Status

- **Neu laden**. Aktualisiert die in der Tabelle dargestellten Daten.
- **Update**. Aktualisiert die entsprechenden Clients auf die neueste verfügbare Version.

Malware-Status

- **Infizierte Ziele scannen**. Führt einen vorkonfigurierten vollständigen Scan derjenigen Ziele aus, die als infiziert angezeigt werden.
- **Löschen**. Löscht die infizierten Dateien von den Zielen.
- **Neu laden**. Aktualisiert die in der Tabelle dargestellten Daten.

Upgrade-Status

- **Upgrade durchführen**. Ersetzt alte Endpunkt-Clients durch die neuesten verfügbaren Produkte.
- **Neu laden**. Aktualisiert die in der Tabelle dargestellten Daten.

7.5. Berichte speichern

Standardmäßig werden geplante Berichte automatisch im Control Center gespeichert.

Wenn Sie Berichte über einen längeren Zeitraum hin benötigen, können Sie sie auf Ihrem Computer abspeichern. Die Zusammenfassung des Berichts ist im PDF-Format verfügbar; die Berichtsdetails sind jedoch nur im CSV-Format verfügbar.

Sie können Berichte auf zweierlei Weise speichern:

- Exportieren
- Download

7.5.1. Berichte exportieren

So exportieren Sie den Bericht auf Ihren Computer:

1. Klicken Sie in der linken unteren Ecke der Berichtseite auf **Exportieren**.
2. Wählen Sie das gewünschte Format für den Bericht:
   - Portabeles Dokumentenformat (PDF) oder
   - Comma-separated values (CSV)
3. Je nach Ihren Browser-Einstellungen wird die Datei automatisch an einen Standard-Speicherort heruntergeladen, oder es wird ein Download-Fenster angezeigt, in dem Sie den Zielordner angeben können.

7.5.2. Berichte herunterladen

Einen Berichtsarchiv enthält sowohl die Zusammenfassung als auch die Details eines Berichts.

So laden Sie ein Berichtsarchiv herunter:

1. Gehen Sie zur Seite **Berichte**.
2. Wählen Sie den Bericht, den Sie speichern möchten.

3. Klicken Sie auf die Schaltfläche **Herunterladen** und wählen Sie entweder **Letzte Instanz**, um die zuletzt erstellte Instanz des Berichts herunterzuladen, oder **Vollständiges Archiv**, um ein Archiv herunterzuladen, das sämtliche Instanzen enthält.

   Je nach Ihren Browser-Einstellungen wird die Datei automatisch an einen Standard-Speicherort heruntergeladen, oder es wird ein Download-Fenster angezeigt, in dem Sie den Zielordner angeben können.

7.6. Berichte per E-Mail versenden

Sie können Berichte mit den folgenden Optionen per E-Mail versenden:

1. Um einen Bericht, den Sie gerade anzeigen, per E-Mail zu versenden, klicken Sie auf die Schaltfläche **E-Mail** in der linken unteren Ecke der Berichtsseite. Der Bericht wird an die mit Ihrem Konto verknüpften E-Mail-Adresse gesendet.
2. So konfigurieren Sie den Versand geplanter Berichte per E-Mail:
   a. Gehen Sie zur Seite **Berichte**.
   b. Klicken Sie auf den gewünschten Berichtnamen.
   c. Wählen Sie unter **Optionen > Zustellung** den Punkt **Per E-Mail senden an**.
   d. Geben Sie die gewünschte E-Mail-Adresse im Feld darunter ein. Sie können beliebig viele E-Mail-Adressen hinzufügen.
   e. Klicken Sie auf **Speichern**.

> **Beachten Sie**
> In der PDF-Datei, die per E-Mail gesendet wird, sind nur die Berichtszusammenfassung und das Diagramm enthalten. Die Berichtsdetails sind in der CSV-Datei enthalten.

7.7. Berichte ausdrucken

Das Control Center verfügt derzeit über keine Druckoptionen. Um einen Bericht zu drucken, müssen Sie ihn zunächst auf Ihrem Computer speichern.

8. QUARANTÄNE

Die Quarantäne ist ein verschlüsselter Ordner, in dem potenziell bösartige Dateien aufbewahrt werden, so zum Beispiel vermutlich oder tatsächlich mit Malware infizierte Dateien und andere unerwünschte Dateien. Die in der Quarantäne enthaltenen Dateien können weder ausgeführt noch geöffnet werden, Viren oder andere Malware können also keinen Schaden mehr anrichten.

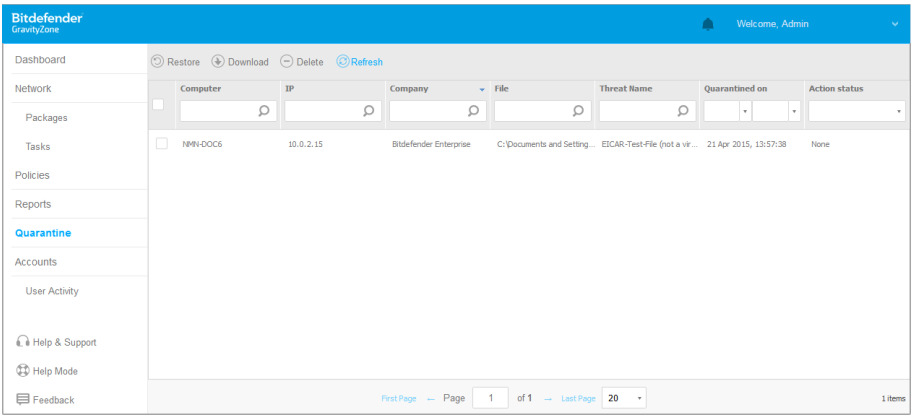
GravityZone verschiebt Dateien gemäß den Richtlinien, die Endpunkten zugewiesen wurden, in die Quarantäne. Standardmäßig werden Dateien, die nicht desinfiziert werden können, in die Quarantäne verschoben.

Jeder Endpunkt hat seine eigene lokale Quarantäne.

Dateien in Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Malware-Forschern analysiert werden können. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen. Zudem werden die Dateien in Quarantäne nach jedem Update der Malware-Signaturen gescannt. Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt. Diese Funktionen beziehen sich auf die einzelnen Sicherheitsrichtlinien auf der Seite **Richtlinien**, und Sie können sie entweder beibehalten oder deaktivieren. Weitere Informationen finden Sie unter „Quarantäne“ (S. 101).

8.1. Die Quarantäne im Detail

Auf der **Quarantäne**-Seite finden sich detaillierte Informationen zu allen Dateien, die von allen Endpunkten, die Sie verwalten, in die Quarantäne verschoben wurden.



Die Quarantäneübersicht

Informationen über Dateien in Quarantäne werden in einer Tabelle angezeigt. Je nach Anzahl der verwalteten Endpunkte und dem Ausmaß vergangener Infektionen kann die Quarantäne-Tabelle unter Umständen sehr viele Einträge enthalten. Die Tabelle kann über mehrere Seiten gehen (pro Seite werden standardmäßig nur 20 Einträge angezeigt).

Verwenden Sie die Navigationsschaltflächen am unteren Rand der Tabelle, um zwischen den Seiten zu wechseln. Um die Anzahl der Einträge zu ändern, die pro Seite angezeigt werden, wählen Sie die entsprechende Option aus dem Menü neben den Navigationsschaltflächen aus.

Um leichter an die gewünschten Informationen zu gelangen, können Sie Suchbegriffe in die Suchfelder der Spaltenüberschriften eingeben. Sie können beispielsweise nach einer bestimmten Bedrohung suchen, die im Netzwerk gefunden wurde, oder nach einem bestimmten Netzwerkobjekt. Sie können auch auf die Spaltenüberschriften klicken, um Daten nach einer bestimmten Spalte zu ordnen.

Um sicherzustellen, dass die neuesten Informationen angezeigt werden, klicken Sie am oberen Rand der Tabelle auf **Neu laden**. Dies könnte notwendig werden, wenn Sie mehr Zeit auf der Seite verbringen.

8.2. Quarantäne für Computer und virtuelle Maschinen

8.2.1. Quarantäne-Details anzeigen

Die Quarantäne-Tabelle enthält die folgenden Informationen:

- Der Name des Endpunktes, auf dem die Bedrohung gefunden wurde.
- IP-Adresse des Endpunktes, auf dem die Bedrohung gefunden wurde.
- Pfad zu der infizierten oder verdächtigen Datei auf dem Endpunkt, auf dem sie gefunden wurde.
- Der Name, den die Bitdefender-Sicherheitsexperten der Malware-Bedrohung gegeben haben.
- Zeitpunkt, zu dem die Datei in die Quarantäne verschoben wurde.
- Der Status der Aktion, die auf die in die quarantäneverschobene Datei angewendet werden sollte.

8.2.2. Verwalten von Dateien in der Quarantäne

Die Quarantäne verhält sich je nach Umgebung etwas unterschiedlich:

- **Security for Endpoints** speichert die in die Quarantäne verschobenen Dateien auf jedem verwalteten Computer. Über das Control Center können Sie einzelne Dateien in der Quarantäne löschen oder wiederherstellen.
- **Security for Virtualized Environments (Multi-Plattform)** speichert die in die Quarantäne verschobenen Dateien auf jeder verwalteten virtuellen Maschine. Über das Control Center können Sie einzelne Dateien in der Quarantäne löschen oder wiederherstellen.

Dateien aus der Quarantäne wiederherstellen

Es kann vorkommen, dass Sie Dateien in Quarantäne an ihrem Ursprungsort oder an anderer Stelle wiederherstellen müssen. So zum Beispiel, wenn Sie wichtige Dateien wiederherstellen möchten, die einem infizierten Archiv gespeichert sind, das in Quarantäne verschoben wurde.

Beachten Sie
Die Wiederherstellung von Dateien aus der Quarantäne ist nur in Umgebungen möglich, die durch Security for Endpoints und Security for Virtualized Environments (Multi-Plattform) geschützt sind.

Um eine oder mehrere Dateien in Quarantäne wiederherzustellen:

1. Öffnen Sie die **Quarantäne**-Seite.
2. Markieren Sie die Kästchen für die Dateien in Quarantäne, die Sie wiederherstellen möchten.
3. Klicken Sie auf die Schaltfläche **Wiederherstellen** am oberen Rand der Tabelle.
4. Wählen Sie den Speicherort aus, an dem Sie die ausgewählten Dateien wiederherstellen möchten (entweder der ursprüngliche Speicherort oder ein benutzerdefinierter Speicherort auf dem Ziel-Computer).

   Wenn die Wiederherstellung an einem benutzerdefinierten Speicherort stattfinden soll, müssen Sie den absoluten Pfad in das entsprechende Feld eingeben.
5. Wählen Sie **Ausschluss automatisch zur Richtlinie hinzufügen**, um die wiederherzustellenden Dateien von zukünftigen Scans auszuschließen. Der Ausschluss gilt für alle Richtlinien, die sich auf die gewählten Dateien beziehen, außer auf die Standardrichtlinie - diese kann nicht verändert werden.
6. Klicken Sie auf **Speichern**, um die Aktion zum Wiederherstellen einer Datei anzufordern. Der Status "Ausstehend" wird in der Spalte **Aktion** angezeigt.
7. Die angeforderte Aktion wird sofort an die Ziel-Endpunkte geschickt bzw. sobald diese wieder online sind.

   Auf der Seite **Aufgaben** werden Details zum Status der Aktion angezeigt. Sobald eine Datei wiederhergestellt ist, wird der entsprechende Eintrag in der Quarantäne-Tabelle nicht mehr auftauchen.

Dateien in der Quarantäne automatisch löschen

Standardmäßig werden Dateien in der Quarantäne, die älter als 30 Tage sind, automatisch gelöscht. Sie können diese Einstellung ändern, indem Sie die den verwalteten Endpunkten zugewiesene Richtlinie bearbeiten.

Um das Intervall für die automatische Löschung von Dateien in Quarantäne zu ändern:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Identifizieren Sie die Richtlinie, die den Endpunkten zugewiesen wurde, auf denen Sie die Einstellung ändern möchten, und klicken Sie auf ihren Namen.
3. Gehen Sie zur Seite **Malware-Schutz > Einstellungen**.
4. Wählen Sie im Bereich **Quarantäne** die Anzahl an Tagen, nach denen Dateien in der Quarantäne gelöscht werden sollen.
5. Klicken Sie **Speichern**, um die Änderungen zu speichern.

Dateien in der Quarantäne manuell löschen

Wenn Sie Dateien in der Quarantäne von Hand löschen möchten, sollten Sie zunächst sicherstellen, dass die von Ihnen ausgewählten Dateien nicht mehr gebraucht werden.

Eine Datei kann unter Umständen auch selbst die Malware sein. Sollten Ihre Nachforschungen dies ergeben, können Sie die Quarantäne nach dieser speziellen Bedrohung durchsuchen und sie aus der Quarantäne löschen.

Um eine oder mehrere Dateien in Quarantäne zu löschen:

1. Öffnen Sie die **Quarantäne**-Seite.
2. Markieren Sie die Kästchen für die Dateien in der Quarantäne, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche ⊖ **Löschen** am oberen Rand der Tabelle. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

   Der Status "Ausstehend" wird in der Spalte **Aktion** angezeigt.

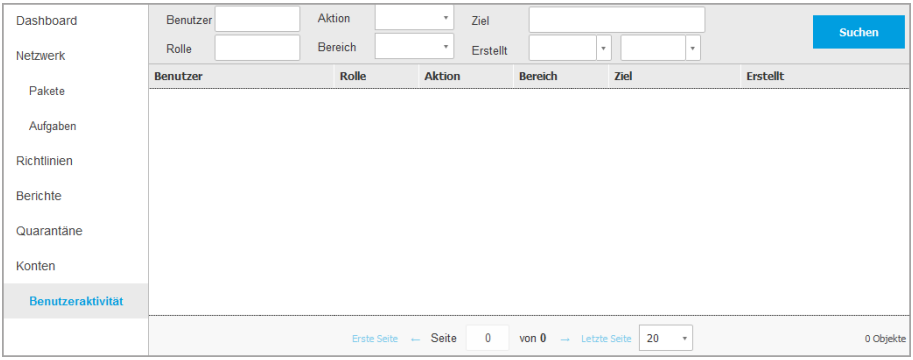
   Die angeforderte Aktion wird sofort (bzw. sobald diese wieder online sind) an die entsprechenden Netzwerkobjekte geschickt. Sobald eine Datei gelöscht wurde, wird der entsprechende Eintrag in der Quarantäne-Tabelle nicht mehr auftauchen.

9. BENUTZERAKTIVITÄTSPROTOKOLL

Das Control Center protokolliert alle von Benutzer ausgeführten Operationen und Aktionen. Die Benutzeraktivitätsliste enthält je nach Ihren Administratorrechten die folgenden Ereignisse:

- Anmelden und Abmelden
- Berichte erstellen, bearbeiten, umbenennen und löschen
- Dashboard-Portlets hinzufügen und entfernen
- Zugangsdaten erstellen, bearbeiten und löschen
- Netzwerkpakete erstellen, modifizieren, herunterladen und löschen
- Netzwerkaufgaben erstellen
- Benutzerkonten erstellen, bearbeiten, umbenennen und löschen
- Endpunkte löschen oder zwischen Gruppen verschieben
- Gruppen erstellen, verschieben, umbenennen und löschen
- Dateien aus der Quarantäne löschen oder wiederherstellen
- Benutzerkonten erstellen, bearbeiten und löschen
- Richtlinien erstellen, bearbeiten, umbenennen, zuweisen und löschen

Details zu den Aktivitäten der Benutzer finden Sie auf der Seite **Konten > Benutzeraktivität**.



Die Seite Benutzeraktivität

Um aufgezeichnete Ereignisse anzuzeigen, an denen Sie interessiert sind, müssen Sie eine Suche definieren. Geben Sie die Suchkriterien in die verfügbaren Felder ein und klicken Sie auf **Suchen**. Alle zu Ihren Kriterien passenden Einträge werden in der Tabelle angezeigt.

Die Spalten geben nützliche Informationen zu den aufgelisteten Ereignissen:

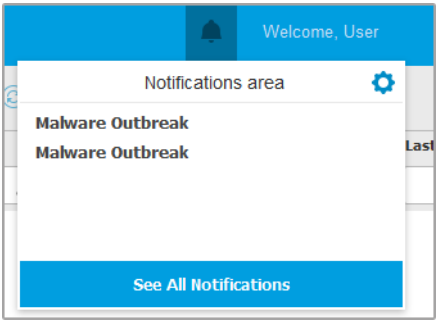
- Der Name des Benutzers, der die Aktion durchgeführt hat.
- Benutzerrolle.
- Aktion, die das Ereignis ausgelöst hat.
- Art des Konsolenobjekts, das von der Aktion betroffen ist.
- Bestimmtes Konsolenobjekt, das von der Aktion betroffen ist.
- Zeitpunkt, zu dem das Ereignis eingetreten ist.

Um Ereignisse nach einer Spalte zu ordnen, klicken Sie einfach auf die Überschrift der jeweiligen Spalte. Klicken Sie erneut auf die Spaltenüberschrift, um die Sortierungsreihenfolge umzukehren.

Um Details zu einem Ereignis anzuzeigen, wählen Sie es aus und sehen Sie in den Abschnitt unter der Tabelle.

10. BENACHRICHTIGUNGEN

Je nach den Ereignissen, die in Ihrem Netzwerk auftreten, wird das Control Center verschiedene Benachrichtigungen anzeigen, die Sie über den Sicherheitsstatus Ihrer Umgebung auf dem Laufenden halten. Die Benachrichtigungen werden im **Infobereich** in der oberen rechten Ecke des Control Center angezeigt.



Infobereich

Wenn neue Ereignisse im Netzwerk gefunden werden, wird im Infobereich ein rotes Symbol 11 angezeigt, das die Zahl der neu gefundenen Ereignisse angibt. Klicken Sie auf das Symbol, um eine Liste der gefundenen Ereignisse anzuzeigen.

10.1. Benachrichtigungsarten

Hier eine Liste der verfügbaren Benachrichtigungstypen:

Malware-Ausbruch

Diese Benachrichtigung wird an Benutzer gesendet, die mindestens 5 % ihrer verwalteten Netzwerkobjekte mit derselben Malware infiziert haben.

Sie können die Malware-Ausbruchschwelle im Fenster **Benachrichtigungseinstellungen** konfigurieren. Weitere Informationen finden Sie unter „Benachrichtigungseinstellungen konfigurieren“ (S. 163).

Lizenz läuft ab

Diese Benachrichtigung wird 30, 7 und dann noch einmal einen Tag bevor die Lizenz abläuft, gesendet.

Die Benutzergrenze der Lizenz ist erreicht
Diese Benachrichtigung wird gesendet, wenn alle verfügbaren Lizenzen vergeben sind.

Benutzergrenze der Lizenz ist bald erreicht
Diese Benachrichtigung wird gesendet, wenn 90 % der verfügbaren Lizenzen vergeben sind.

Update verfügbar
Diese Benachrichtigung informiert Sie über ein neues zur Verfügung stehendes GravityZone-Update.

Phishing-Schutz-Ereignis
Diese Benachrichtigung wird jedes Mal ausgegeben, wenn der Endpunkt-Agent den Zugriff auf eine bekannte Phishing-Webseite blockiert. Die Benachrichtigungen enthält auch Details wie den Endpunkt, von dem aus versucht wurde, auf die unsichere Webseite zuzugreifen (Name und IP-Adresse), den installierten Agent oder die blockierte URL.

Firewall-Ereignis
Diese Benachrichtigung wird jedes Mal ausgegeben, wenn das Firewall-Modul eines installierten Agenten einen Port-Scan oder den Zugriff einer Anwendung auf das Netzwerk gemäß der zugewiesenen Richtlinie blockiert hat.

AVC/IDS-Ereignis
Diese Benachrichtigung wird jedes Mal ausgegeben, wenn eine potenziell gefährliche Anwendung auf einem Endpunkt in Ihrem Netzwerk gefunden und blockiert wurde. Details zur Art der gefährlichen Anwendung sowie Name und Pfad werden auch angezeigt.

Benutzersteuerungsereignis
Diese Benachrichtigung wird jedes Mal ausgegeben, wenn der Endpunkt-Client gemäß der zugewiesenen Richtlinie Benutzeraktivitäten wie das Browsen im Internet oder eine Software-Anwendung blockiert.

Identitätsschutzereignis
Diese Benachrichtigung wird jedes Mal ausgegeben, wenn gemäß den Identitätsschutzregeln Datenverkehr auf einem Endpunkt blockiert wird.

Produkt-Modul-Ereignis
Diese Benachrichtigung wird jedes Mal ausgegeben, wenn ein Sicherheitsmodul eines installierten Agenten deaktiviert wird.

Produktregistrierungsereignis

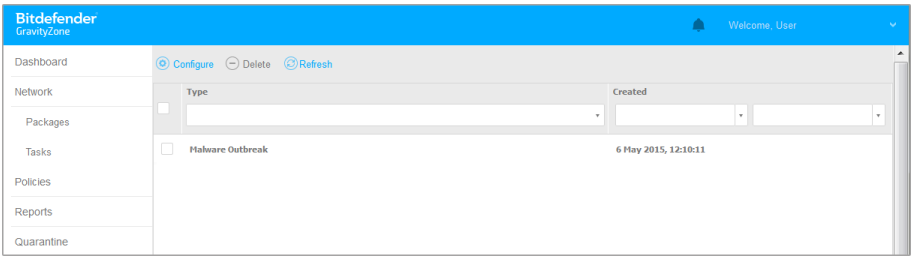
Diese Benachrichtigung informiert Sie darüber, wenn sich der Registrierungsstatus eines in Ihrem Netzwerk installierten Agenten geändert hat.

Anmeldung von einem neuen Gerät

Diese Benachrichtigung informiert Sie darüber, dass über Ihr GravityZone-Konto eine Anmeldung am Control Center von einem Gerät aus erfolgt ist, von dem aus Sie sich bisher noch nicht angemeldet hatten.

10.2. Benachrichtigungen anzeigen

Sie können die Benachrichtigungen anzeigen, indem Sie auf die Schaltfläche **Infobereich** und anschließend auf **Alle Benachrichtigungen anzeigen** klicken. Eine Tabelle mit allen Benachrichtigungen wird angezeigt.



Die Benachrichtigungsübersicht

Abhängig von der Anzahl der Benachrichtigungen kann sich die Tabelle über mehrere Seiten erstrecken (standardmäßig werden nur 20 Einträge pro Seite angezeigt).

Verwenden Sie die Navigationsschaltflächen am unteren Rand der Tabelle, um zwischen den Seiten zu wechseln.

Um die Anzahl der Einträge zu ändern, die pro Seite angezeigt werden, wählen Sie die entsprechende Option aus dem Menü neben den Navigationsschaltflächen aus.

Sollten zu viele Einträge angezeigt werden, können Sie die Suchfelder unterhalb der Spaltenüberschriften oder das Filtermenü über der Tabelle verwenden, um die angezeigten Daten zu filtern.

- Sie können die Benachrichtigungen Filtern, indem Sie den gewünschten Benachrichtigungstyp aus dem Menü **Typ** wählen. Optional können Sie auch den Zeitraum, in dem die Benachrichtigungen erstellt wurden, eingrenzen, um

die Zahl der in der Tabelle angezeigten Einträge zu verringern, besonders wenn sehr viele Benachrichtigungen erstellt worden sind.

- Wenn Sie auf den Namen einer Benachrichtigung in der Tabelle klicken, werden weitere Details zu ihr angezeigt. Unter der Tabelle wird der Bereich **Details** angezeigt, in dem das Ereignis angezeigt wird, dass die Benachrichtigung verursacht hat.

10.3. Benachrichtigungen löschen

So löschen Sie Benachrichtigungen:

1. Klicken Sie auf die Schaltfläche **Infobereich** auf der rechten Seite der Menüleiste und anschließend auf **Alle Benachrichtigungen anzeigen**. Eine Tabelle mit allen Benachrichtigungen wird angezeigt.
2. Wählen Sie die Benachrichtigungen, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen** am oberen Rand der Tabelle.

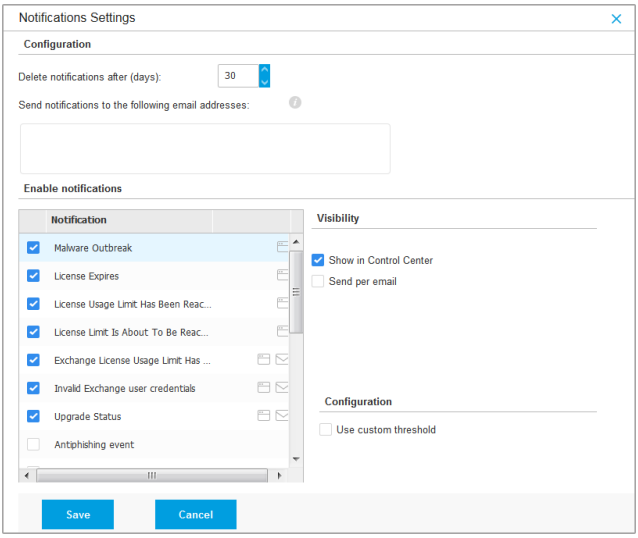
Sie können auch einstellen, dass Benachrichtigungen nach einer bestimmten Anzahl an Tagen gelöscht werden. Weitere Informationen finden Sie unter „Benachrichtigungseinstellungen konfigurieren“ (S. 163).

10.4. Benachrichtigungseinstellungen konfigurieren

Die Benachrichtigungstypen, die gesendet werden, sowie die E-Mail-Adresse, an die sie gesendet werden, können für jeden Benutzer einzeln festgelegt werden.

So konfigurieren Sie die Benachrichtigungseinstellungen:

1. Klicken Sie auf die Schaltfläche **Infobereich** auf der rechten Seite der Menüleiste und anschließend auf **Alle Benachrichtigungen anzeigen**. Eine Tabelle mit allen Benachrichtigungen wird angezeigt.
2. Klicken Sie auf die Schaltfläche **Konfigurieren** am oberen Rand der Tabelle. Das Fenster **Benachrichtigungsseinstellungen** wird angezeigt.



Benachrichtigungseinstellungen

Beachten Sie
Sie können das Fenster für die **Benachrichtigungseinstellungen** auch direkt über das **Konfigurieren**-Symbol oben rechts im **Infobereich**-Fenster aufrufen.

3. Im Bereich **Konfiguration** können Sie die folgenden Einstellungen vornehmen:
   - Sie können einstellen, dass Benachrichtigungen nach einer bestimmten Anzahl an Tagen gelöscht werden. Geben Sie die gewünschte Anzahl an Tagen in das Feld **Benachrichtigungen löschen nach (Tagen)** ein.
   - Wenn Sie möchten, können Sie die Benachrichtigungen per E-Mail an eine bestimmte E-Mail-Adresse senden lassen. Geben Sie die E-Mail-Adressen in das dafür vorgesehene Feld ein; drücken Sie die `Eingabetaste` zwischen mehreren Adressen.
4. Im Bereich **Benachrichtigung aktivieren** können Sie festlegen, welche Art von Benachrichtigungen Sie von GravityZone erhalten möchten. Sie können auch für jeden Benachrichtigungstyp einzeln die Anzeige- und Versandoptionen festlegen.

Wählen Sie einen Benachrichtigungstyp aus der Liste. Weitere Informationen finden Sie unter „Benachrichtigungsarten“ (S. 160). Solange ein Benachrichtigungstyp ausgewählt ist, können Sie auf der rechten Seite die Optionen (sofern vorhanden) für diesen Typ konfigurieren:

Transparenz

- **Im Control Center anzeigen**: dieser Ereignistyp wird im Control Center mithilfe des Symbols im **Infobereich** angezeigt.
- **per E-Mail senden**: Dieser Ereignistyp wird auch an bestimmte E-Mail-Adressen gesendet. In diesem Fall müssen Sie die E-Mail-Adressen in das entsprechende Feld eingeben und nach jeder Adresse die `Enter-Taste` drücken.

Konfiguration

- **Benutzerdefinierte Schwelle verwenden** - hiermit kann eine Schwelle für die eingetretenen Ereignisse festgelegt werden, für die die ausgewählte Benachrichtigung gesendet wird.

  Zum Beispiel wird die Malware-Ausbruch-Benachrichtigung standardmäßig an Benutzer gesendet, die mindestens 5 % ihrer verwalteten Netzwerkobjekte mit der gleichen Malware infiziert haben. Sie können die Malware-Ausbruchschwelle verändern, indem Sie die Option **Benutzerdefinierte Schwelle verwenden** aktivieren und dann den gewünschten Wert in das Feld **Malware-Ausbruchschwelle** eingeben.
- Für **Aufgabenstatus** können Sie den Typ des Status wählen, der diesen Typ von Benachrichtigung auslöst:
  - **Jeden Status** - gibt jedes Mal eine Benachrichtigung aus, wenn eine vom Control Center gesendete Aufgabe ausgeführt wurde, unabhängig vom Status.
  - **Nur fehlgeschlagene** – gibt jedes Mal eine Benachrichtigung aus, wenn eine vom Control Center gesendete Aufgabe fehlgeschlagen ist.

5. Klicken Sie auf **Speichern**.

11. HILFE ERHALTEN

Bitdefender hat es sich zur Aufgabe gemacht, seinen Kunden beispiellos schnellen und sorgfältigen Support zu bieten. Sollten Probleme im Zusammenhang mit Ihrem Bitdefender-Produkt auftreten oder Sie Fragen dazu haben, so wenden Sie sich bitte an unser Online-Support-Center. Dort gibt es verschiedene Ressourcen, mit deren Hilfe Sie schnell die richtige Lösung oder Antwort finden können. Sie können auch das Kundenbetreuungs-Team von Bitdefender kontaktieren. Unsere Kundenbetreuer beantworten Ihre Fragen zügig und bieten Ihnen die benötigte Unterstützung.

Beachten Sie
Im Support-Center finden Sie weiterführende Informationen zu unseren Support-Leistungen und Support-Richtlinien.

11.1. Bitdefender-Support-Center

Im Bitdefender-Support-Center finden Sie alle Hilfe und Informationen rund um Ihr Bitdefender-Produkt.

Dabei stehen Ihnen verschiedene Ressourcen zur Verfügung, um die richtige Lösung oder Antwort zu finden:

- Artikel in der Wissensdatenbank
- Bitdefender-Support-Forum
- Produktdokumentation

Zudem können Sie auch Ihre favorisierte Suchmaschine nutzen, um mehr zu erfahren über Computersicherheit, die Bitdefender-Produkte und das Unternehmen.

Artikel in der Wissensdatenbank

Die Bitdefender-Wissensdatenbank ist eine Online-Datenbank mit Informationen rund um die Bitdefender-Produkte. Hier sind in einem leicht zugänglichen Format Berichte zu den Ergebnissen des fortlaufenden technischen Supports sowie der Bugfix-Aktivitäten der Bitdefender-Support- und Entwicklungsteams gespeichert. Hinzu kommen Artikel zur Virenvorbeugung, detaillierte Erklärungen zur Verwaltung von Bitdefender-Lösungen und vieles mehr.

Die Bitdefender-Wissensdatenbank ist öffentlich zugänglich und komplett durchsuchbar. Die darin enthaltenen Informationen sind äußerst umfangreich und

stellen eine weitere Methode dar, mit der Bitdefender-Kunden mit dem notwendigen technischen Wissen versorgt werden. Alle berechtigen Informationsanfragen oder Fehlermeldungen von Bitdefender-Kunden finden sich über kurz oder lang im Bitdefender-Wissensdatenbank wieder und dienen als Bugfix-Anleitungen, Umgehungslösungen oder Informationsartikel, die die Hilfedateien des Produkts ergänzen sollen.

Die Bitdefender-Wissensdatenbank für Unternehmensprodukte steht Ihnen jederzeit unter http://www.bitdefender.de/support/business.html zur Verfügung.

Bitdefender-Support-Forum

Das Bitdefender-Support-Forum bietet Bitdefender-Anwendern eine Möglichkeit, schnelle Hilfe zu erhalten oder anderen Hilfestellung zu geben. Hier können Sie Ihre Probleme und Fragen rund um Ihr Bitdefender-Produkt posten.

Support-Techniker von Bitdefender überwachen neue Einträge in das Forum, um Ihnen helfen zu können. Außerdem können Sie eine Antwort auf Ihre Frage oder einen Lösungsvorschlag von einem bereits erfahrenen Bitdefender-Anwender erhalten.

Bevor Sie einen Eintrag ins Forum stellen, suchen Sie bitte im Forum nach einem ähnlichen oder verwandten Themenbereich.

Das Bitdefender Support-Forum finden Sie unter http://forum.bitdefender.com. Es steht in 5 verschiedenen Sprachen zur Verfügung: Englisch, Deutsch, Französisch, Spanisch und Rumänisch. Mit einem Klick auf **Business Protection** gelangen Sie in den Bereich Unternehmensprodukte.

Produktdokumentation

Die Produktdokumentation ist die umfassendste Informationsquelle rund um Ihr Produkt.

Die neuesten Versionen der Dokumentation für Bitdefender-Unternehmensprodukte finden Sie im Support Center im Bereich **Dokumentation** der jeweiligen Produktseite.

11.2. Hilfe anfordern

Nutzen Sie das Online-Support-Center, um Unterstützung anzufordern:

1. Gehen Sie zu http://www.bitdefender.de/support/contact-us.html.

2. Im Kontaktformular können Sie ein E-Mail-Support-Ticket eröffnen oder auf weitere Kontaktoptionen zugreifen.

11.3. Verwenden des Support-Tools

Das Support-Tool von GravityZone ermöglicht Benutzern und Support-Mitarbeitern den schnellen Zugriff auf alle Informationen, die Sie zur Lösung von Problemen benötigen. Führen Sie das Support-Tool auf den betroffenen Computern aus und senden Sie das daraufhin erstellte Archiv mit den Informationen für die Fehlersuche an einen Bitdefender-Support-Mitarbeiter.

11.3.1. Das Support-Tool unter Windows verwenden

1. Laden Sie das Support-Tool herunter und bringen Sie sie auf die betroffenen Computer aus. Um das Support-Tool herunterzuladen:
   a. Bauen Sie über Ihr Konto eine Verbindung mit der Control Center auf.
   b. Klicken Sie in der unteren linken Bildschirmecke der Konsole auf **Hilfe und Support**.
   c. Die Download-Links finden Sie im **Support**-Bereich. Es stehen zwei Versionen zur Verfügung: eine für 32-Bit-Systeme und eine für 64-Bit-Systeme. Stellen Sie sicher, dass Sie die richtige Version verwenden, wenn Sie das Support-Tool auf einem Computer ausführen.
2. Führen Sie das Support-Tool lokal auf jedem der betroffenen Computer aus.
   a. Markieren Sie das Zustimmungskästchen und klicken Sie auf **Weiter**.
   b. Geben Sie in das Formular die nötigen Daten ein:
      i. Geben Sie Ihre E-Mail-Adresse ein.
      ii. Geben Sie Ihren Namen ein.
      iii. Wählen Sie Ihr Land aus dem entsprechenden Menü.
      iv. Beschreiben Sie im Textfeld das Problem, das aufgetreten ist.
      v. Sie können auch versuchen das Problem zu reproduzieren, bevor Sie mit der Datensammlung beginnen. Gehen Sie in diesem Fall folgendermaßen vor:
         A. Aktivieren Sie die Option **Versuchen Sie, das Problem vor der Übertragung zu reproduzieren**.

B. Klicken Sie auf **Weiter**.

C. Wählen Sie die Art des aufgetretenen Problems.

D. Klicken Sie auf **Weiter**.

E. Reproduzieren Sie das Problem auf Ihrem Computer. Kehren Sie danach zum Support-Tool zurück und wählen Sie die Option **Ich habe das Problem reproduziert**.

c. Klicken Sie auf **Weiter**. Das Support Tool sammelt Produktinformationen, Informationen zu anderen Anwendungen, die auf ihrem System installiert sind sowie die Software und Hardware Konfiguration.

d. Warten Sie, bis der Vorgang beendet ist.

e. Klicken Sie auf **Beenden**, um das Fenster zu schließen. Es wurde ein ZIP-Archiv auf Ihrem Desktop erstellt.

Schicken Sie das ZIP-Archiv gemeinsam mit Ihrer Anfrage an einen Bitdefender-Support-Mitarbeiter. Verwenden Sie dafür das E-Mail-Support-Ticket-Formular auf der **Hilfe und Support**-Seite der Konsole.

11.3.2. Das Support-Tool unter Linux

Für Linux-Betriebssysteme ist das Support-Tool im Bitdefender-Sicherheitsagenten integriert.

Linux-Systeminformationen können Sie über das Support-Tool mit dem folgendem Befehl erhalten:

```
# /opt/BitDefender/bin/bdconfigure
```

Dabei stehen folgende Optionen zur Verfügung:

- `--help` zeigt eine Liste aller Support-Tool-Befehle an.
- `enablelogs` aktiviert Produkt- und Kommunikationsmodulprotokolle (alle Dienste werden automatisch neu gestartet).
- `disablelogs` deaktiviert Produkt- und Kommunikationsmodulprotokolle (alle Dienste werden automatisch neu gestartet).
- `deliverall` erstellt ein Archiv, das die Produkt- und Kommunikationsmodulprotokolle enthält. Es wird an den Ordner `/tmp` im

folgenden Format zugestellt: `bitdefender_Maschinenname_Zeitstempel.tar.gz`.

1. Wenn Sie die Protokolle deaktivieren möchten, werden Sie um eine Bestätigung gebeten. Wenn nötig, werden die Dienste automatisch neu gestartet.
2. Wenn Sie Protokolle löschen möchten, werden Sie um eine Bestätigung gebeten.

- `deliverall -default` lLiefert dieselben Informationen wie die vorige Option, aber Standardaktionen werden auf die Protokolle ausgeführt, ohne dass der Benutzer dies bestätigt (die Protokolle werden deaktiviert und gelöscht).

So melden Sie ein GravityZone-Problem, das Ihre Linux-Systeme beeinträchtigt (verwenden Sie dazu die oben beschriebenen Optionen):

1. Aktivieren Sie Produkt- und Kommunikationsmodulprotokolle.
2. Versuchen Sie, das Problem nachzustellen.
3. Deaktivieren Sie Protokolle.
4. Erstellen Sie ein Protokollarchiv.
5. Öffnen Sie ein E-Mail-Support-Ticket über das Formular auf der Seite **Hilfe & Support** des Control Center; geben Sie eine Beschreibung des Problems ein und hängen Sie das Protokollarchiv an.

Das Support-Tool für Linux liefert die folgenden Informationen:

- Die Ordner `etc`, `var/log`, `/var/crash` (sofern vorhanden) und `var/epag` von `/opt/BitDefender`; darin sind die Bitdefender-Protokolle und -Einstellungen enthalten.
- Die Datei `/tmp/bdinstall.log`, die Installationsinformationen enthält.
- Die Datei `network.txt`, die Netzwerkeinstellungen und Informationen zur Netzwerkverbindung der Maschine enthält.
- Die Datei `system.txt`, die allgemeine Systeminformationen enthält (Distribution und Kernel-Version, verfügbarer RAM und freier Festplattenspeicher)
- Die Datei `users.txt`, die Benutzerinformationen enthält
- Andere Informationen zum Produkt im Zusammenhang mit dem Systen, z. B. externe Verbindungen von Prozessen und CPU-Auslastung

- Systemprotokolle

11.4. Kontaktinformation

Effiziente Kommunikation ist der Schlüssel zu einem erfolgreichen Unternehmen. Seit mehr als 10 Jahren überbietet Bitdefender konstant die bereits hochgesteckten Erwartungen seiner Kunden und Partner und diese Tradition wollen wir auch in Zukunft fortführen. Für jedwede Fragen stehen wir Ihnen gerne zur Verfügung.

11.4.1. Internet-Adressen

Vertrieb: enterprisesales@bitdefender.com
Support-Center:http://www.bitdefender.de/support/business.html
Dokumentation: documentation@bitdefender.com
Lokale Vertriebspartner:http://www.bitdefender.de/partners
Partnerprogramm: partners@bitdefender.com
Presse: presse@bitdefender.de
Virus-Einsendungen: virus_submission@bitdefender.com
Spam-Einsendungen: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Website:http://www.bitdefender.de

11.4.2. Händler vor Ort

Bitdefender-Händler stehen für vertriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung.

So finden Sie einen Bitdefender-Händler in Ihrem Land:

1. Gehen Sie zu http://www.bitdefender.de/partners.
2. Öffnen Sie die **Partner-Suche**.
3. Die Kontaktinformationen zum örtlichen Bitdefender Distributor sollten automatisch eingeblendet werden. Sollte dies nicht der Fall sein, so wählen Sie Ihr Land aus, um die Informationen anzuzeigen.
4. Falls Sie in Ihrem Land keinen Bitdefender-Händler finden, können Sie uns gerne unter enterprisesales@bitdefender.com kontaktieren.

11.4.3. Bitdefender-Niederlassungen

Bitdefender-Niederlassungen stehen Ihnen für betriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Bereichen jederzeit zur Verfügung. Die genauen Kontaktdaten und Adressen finden Sie in der unten stehenden Auflistung.

USA

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Telefon (Vertrieb&Technischer Support): 1-954-776-6262
Vertrieb: sales@bitdefender.com
Web: http://www.bitdefender.com
Support-Center: http://www.bitdefender.com/support/business.html

Frankreich

PROFIL TECHNOLOGY
49, Rue de la Vanne
92120 Montrouge
Fax: +33 (0)1 47 35 07 09
Telefon: +33 (0)1 47 35 72 73
E-Mail: supportpro@profiltechnology.com
Webseite: http://www.bitdefender.fr
Support-Center: http://www.bitdefender.fr/support/professionnel.html

Spain

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Fax: (+34) 93 217 91 28
Telefon (Geschäftsstelle&Vertrieb): (+34) 93 218 96 15
Telefon (Technischer Support): (+34) 93 502 69 10
Vertrieb: comercial@bitdefender.es
Webseite: http://www.bitdefender.es
Support-Center: http://www.bitdefender.es/support/business.html

Deutschland

Bitdefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Telefon (Geschäftsstelle&Vertrieb): +49 (0)2301 91 84 222
Telefon (Technischer Support): +49 (0)2301 91 84 444
Vertrieb: vertrieb@bitdefender.de
Webseite: http://www.bitdefender.de
Support-Center: http://www.bitdefender.de/support/business.html

Großbritannien und Irland

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Telefon (Vertrieb&Technischer Support): +44 (0) 8451-305096
E-Mail: info@bitdefender.co.uk
Vertrieb: sales@bitdefender.co.uk
Webseite: http://www.bitdefender.co.uk
Support-Center: http://www.bitdefender.co.uk/support/business.html

Rumänien

BITDEFENDER SRL
DV24 Offices, Building A
24 Delea Veche Street
024102 Bucharest, Sector 2
Fax: +40 21 2641799
Telefon (Vertrieb&Technischer Support): +40 21 2063470
Vertrieb: sales@bitdefender.ro
Webseite: http://www.bitdefender.ro
Support-Center: http://www.bitdefender.ro/support/business.html

Vereinigte Arabische Emirate

Bitdefender FZ-LLC
Dubai Internet City, Building 17

Office # 160
Dubai, UAE
Telefon (Vertrieb&Technischer Support): 00971-4-4588935 / 00971-4-4589186
Fax: 00971-4-44565047
Vertrieb: sales@bitdefender.com
Web: http://www.bitdefender.com/world
Support-Center: http://www.bitdefender.com/support/business.html

A. Anhänge

A.1. Netzwerkobjekttypen und -status

A.1.1. Netzwerkobjekttypen

Jeder einzelne Objekttyp auf der Seite **Netzwerk** wird durch ein eigenes Symbol dargestellt.

In der folgenden Tabelle sind alle Symbole und dazugehörigen Objekttypen aufgeführt.

Symbol	Typ
	Kundenunternehmen
	Netzwerkgruppe
	Computer
	Relais-Computer
	Virtuelle Maschine
	virtuelle Relais-Maschine

A.1.2. Netzwerkobjektstatus

Jedes Netzwerkobjekt hat einen bestimmten Status in Bezug auf Verwaltungszustand, Sicherheitsprobleme, Netzwerkverbindung usw. In der folgenden Tabelle sind alle Statussymbole und ihre Beschreibung aufgeführt.

Beachten Sie
Die unten stehende Tabelle enthält ein paar generische Statusbeispiele. Dieselben Status können, einzeln oder in Kombination, auch bei anderen Netzwerkobjekttypen wie Netzwerkgruppen, Computer usw. auftreten.

Symbol	Status
	Kundenunternehmen, aktiv, selbstverwaltet
	Kundenunternehmen, aktiv, durch Partner verwaltet
	Kundenunternehmen, gesperrt, selbstverwaltet

Symbol	Status
	Virtuelle Maschine, offline, nicht verwaltet
	Virtuelle Maschine, online, nicht verwaltet
	Virtuelle Maschine, online, verwaltet
	Virtuelle Maschine, online, verwaltet, mit Problemen
	Virtuelle Maschine, gesperrt
	Virtuelle Maschine, gelöscht

A.2. Anwendungsdateitypen

Die Malware-Prüf-Engines von Bitdefender-Sicherheitslösungen können so eingerichtet werden, dass nur Anwendungsdateien geprüft werden. Anwendungsdateien sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen.

Diese Kategorie beinhaltet Dateien mit folgenden Endungen:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; iso; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

A.3. Systemvariablen

Für einige der in der Konsole verfügbaren Einstellungen müssen Sie zunächst den Pfad auf dem Ziel-Computern angeben. Es empfiehlt sich, (nach Möglichkeit) Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist.

Im Folgenden finden Sie eine Liste der vordefinierten Systemvariablen:

`%ALLUSERSPROFILE%`

Der Profilordner für alle Benutzer. Typischer Pfad:

`C:\Dokumente und Einstellungen\Alle Benutzer`

`%APPDATA%`

Der Anwendungsdatenordner des angemeldeten Benutzers. Typischer Pfad:

- Windows XP:

  `C:\Dokumente und Einstellungen\{username}\Anwendungsdaten`

- Windows Vista/7:

  `C:\Benutzer\{username}\AppData\Roaming`

`%HOMEPATH%`

Die Benutzerordner. Typischer Pfad:

- Windows XP:

  `Dokumente und Einstellungen\{username}`

- Windows Vista/7:

  `\Benutzer\{username}`

`%LOCALAPPDATA%`

Temporäre Dateien von Anwendungen. Typischer Pfad:

`C:\Benutzer\{username}\AppData\Lokal`

`%PROGRAMMDATEIEN%`

Der Programmdateienordner. Meist zu finden unter `C:\Programmdateien`.

`%PROGRAMFILES(X86)%`

Der Programme-Ordner für 32-Bit-Anwendungen (auf 64-Bit-Systemen). Typischer Pfad:

`C:\Programmdateien (x86)`

`%COMMONPROGRAMFILES%`

Der Ordner Gemeinsame Dateien. Typischer Pfad:

`C:\Programmdateien\Gemeinsame Dateien`

`%COMMONPROGRAMFILES(X86)%`

Der Ordner Gemeinsame Dateien für 32-Bit-Anwendungen (auf 64-Bit-Systemen). Typischer Pfad:

`C:\Programmdateien (x86)\Gemeinsame Dateien`

`%WINDIR%`

Der Windows SDatenverzeichnis oder SYSROOT. Meist zu finden unter `C:\Windows`.

Glossar

Adware

Adware wird häufig mit einer anderen Anwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware-Anwendungen werden in der Regel installiert, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt, und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

Antivirus-Storm

Eine intensive Beanspruchung von Systemressourcen, die auftritt, wenn Virenschutz-Software gleichzeitig mehrere virtuelle Maschinen auf einem einzigen physischen Host scannt.

Archive

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einem Backup erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

Backdoor (Hintertür)

Eine Sicherheitslücke eines Systems, die der Entwickler oder Administrator absichtlich hinterlässt. Der Grund dafür muss nicht immer bösartig sein. Manche Betriebssysteme haben schon standardmäßig privilegierte Konten eingerichtet, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Befehlszeile

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile

werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

Boot-Sektor:

Der erste Sektor einer Festplatte oder Diskette. Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

Bootvirus

Ein Virus, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert. Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird dieser im Arbeitsspeicher aktiviert. Bei jedem Neustart wird der Virus so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

Cookie

In der Internetbranche werden mit Cookies kleine Dateien bezeichnet, die Daten über einzelne Computer enthalten und die von den Werbetreibenden analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden. Die Cookie-Technologie wird stetig weiterentwickelt mit dem Ziel Benutzern nur noch solche Werbung anzuzeigen, die ihren Interessen entspricht. Für viele ist dies ein zweischneidiges Schwert. Einerseits ist es praktisch, nur Anzeigen zu sehen, an denen man interessiert ist. Anderseits bedeutet es, dass Online-Aktivitäten der Benutzer gewissermaßen auf Schritt und "Klick" verfolgt werden. Es ist also verständlich, dass in diesem Zusammenhang Datenschutz ein umstrittenes Thema ist und viele sich unwohl fühlen, quasi als SKU-Nummer (die Strichcodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden. Auch wenn diese Sicht etwas extrem erscheint, ist sie doch manchmal korrekt.

Dateierweiterung

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind.

Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS. Sie sind gewöhnlich ein bis drei Buchstaben lange (alte Betriebssysteme können oft nicht mehr als drei Buchstaben unterstützen). Beispiele sind "exe" ausführbare Dateien, "ps" für PostScript oder "txt" für Text-Dateien.

Durchsuchen

Kurzform für Web-Browser, ein Programm, mit dem Internetseiten aufgerufen und angezeigt werden können. Die bekanntesten Browser sind Mozilla Firefox und Microsoft Internet Explorer. Beide sind graphische Browser, was bedeutet, dass sie sowohl Grafiken als auch Texte anzeigen können. Weiterhin können die meisten Browser Multimedia-Daten wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

Ereignisanzeige

Ereignisse oder Erscheinungen, die in einem Programm vorkommen. Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

Fehlalarm

Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist.

Heuristik

Eine Methode, um neue Viren zu identifizieren. Diese Scan-Methode benötigt keine spezifischen Virussignaturen. Der Vorteil eines heuristischen Scans ist, dass man nicht von einer neuen Variante eines alten Virus getäuscht werden kann. Manchmal kann jedoch auch ein verdächtiger Code in einem normalen Programm gemeldet werden, ein sogenannter Fehlalarm oder "falsch-positive Meldung" wird angezeigt.

IP

Internet Protocol - Das TCP/IP Protokoll ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.

Keylogger

Ein Keylogger ist eine Anwendung, die alles aufzeichnet, was Sie tippen.

Keylogger sind an sich nicht schädlich. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von Cyber-Kriminellen mit bösartiger Absicht eingesetzt (um beispielsweise private Daten wie Benutzernamen oder Passwörter zu sammeln).

Logdatei (Berichtsdatei)

Eine Datei, die stattgefundene Aktivitäten aufzeichnet. Zum Beispiel speichert Bitdefender eine Prokolldatei mit den gescannten Pfaden, Ordnern, der Anzahl der gescannten Archive und Dateien sowie der Anzahl der gefundenen infizierten oder verdächtigen Dateien.

Makrovirus

Eine Virusform, die in einem Dokument als eingebettetes Makro verschlüsselt wird. Viele Anwendungen, wie Microsoft Word und Excel, unterstützen leistungsstarke Makrosprachen.

Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird.Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

Malware

Malware ist der Sammelbegriff für alle Software-Arten, die darauf ausgelegt sind, Schaden zu verursachen - das Wort setzt sich zusammen aus den englischen Begriffen malicious und software, also bösartige Software. Der Begriff hat sich noch nicht vollständig durchgesetzt, wird aber immer häufiger als Oberbegriff gebraucht, wenn von Viren, Trojanern, Würmern und Malicious Mobile Code die Rede ist.

Malware-Signatur

Malware-Signaturen sind Codebruchstücke, die aus aktuellen Malware-Beispielen extrahiert werden. Diese werden von Antiviren-Programmen zum Musterabgleich und zur Aufspürung von Malware verwendet. Signaturen werden auch genutzt, um den Malware-Code aus infizierten Dateien zu entfernen.

Die Bitdefender Malware-Signatur-Datenbank ist eine Sammlung von stündlich durch Bitdefender-Mitarbeiter upgedateten Malware-Signaturen.

Nicht heuristisch

Diese Scan-Methode beruht auf spezifischen Virussignaturen. Der Vorteil eines nicht-heuristischen Scans ist, dass er nicht von einem Scheinvirus getäuscht werden kann und so Fehlalarme verhindert.

Phishing

Das Senden einer E-Mail an einen Benutzer, in der der Sender sich als Vertreter eines legitimen Unternehmens ausgibt und versucht, den Empfänger so zu manipulieren, dass er persönliche Informationen preisgibt, die dann zum Diebstahl der Identität verwendet werden können. Die E-Mail leitet den Benutzer dann auf eine Webseite, auf der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TANs oder PINs preiszugeben. Es wird oft vorgegeben, dass dies aus Gründen der Aktualisierung geschehen soll. Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

Polymorpher Virus

Ein Virus, der seine Form mit jeder Datei, die er infiziert, ändert. Da diese Viren kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Rootkit

Bei einem Rootkit handelt es sich um eine Sammlung von Software-Tools, mit denen auf ein System mit Administratorrechten zugegriffen werden kann. Der Begriff wurde ursprünglich nur für UNIX-Systeme verwendet und beschrieb rekompilierte Tools, mit denen sich Angreifer Administratorrechte verschaffen und so ihre Anwesenheit vor den tatsächlichen Administratoren verbergen konnten.

Die Hauptaufgabe eines Rootkits besteht darin, Prozesse, Dateien und Protokolle zu verstecken. Sie können auch Daten von Terminals, Netzwerkverbindungen oder Peripheriegeräten abfangen, falls Sie eine entsprechende Software eingebaut haben.

Rootkits sind nicht grundsätzlich schädlich. Einige Systeme und Anwendungen verstecken z. B. wichtige Dateien mithilfe von Rootkits. Sie werden jedoch oft dazu missbraucht, Malware zu verbergen oder unbemerkt einen Eindringling einzuschleusen. In Kombination mit Malware stellen sie eine große Gefahr für Ihr System dar. Denn sie können den Datenverkehr abhören, Sicherheitslücken in Ihrem System schaffen, Dateien und Zugangsdaten verändern, und das alles, ohne entdeckt zu werden.

Schnittstelle

Stelle eines Rechners, an die ein Gerät angeschlossen werden kann. Rechner haben verschiedenartige Schnittstellen. Im Inneren gibt es Schnittstellen zum Anschluss von Festplatten, Grafikkarten und Tastaturen. Extern haben Rechner

Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen. Die Schnittstellennummer gibt die Art der Schnittstelle an. Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Script

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam

Junk-E-Mail oder Junk-Postings in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Spyware

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten über seine Internetverbindung abgreift. Dies geschieht in der Regel zu Werbezwecken. Typischerweise sind Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Shareware-Programmen enthalten, die aus dem Internet heruntergeladen werden können. Die große Mehrzahl von Shareware- und Freeware-Anwendungen ist natürlich frei von Spyware. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an einen Dritten. Spyware kann auch Informationen über E-Mail-Adressen und sogar Passwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Opfer von Spyware wird man oft dann, wenn man sich bestimmte Peer-to-Peer-Dateiaustauschprogramme herunterlädt.

Ganz abgesehen von den Fragen der Ethik und des Datenschutzes belegt Spyware auch unnötig Systemressourcen und Bandbreite, indem über die Internetverbindung des Nutzers Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Symbolleiste

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Task-Leiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Sie enthält kleine Symbole zur Information und zum leichteren Zugriff auf Systemfunktionen wie Drucker, Modems, Lautstärke und anderes. Um auf die Details und Optionen dieser Funktionen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

TCP/IP

Transmission Control Protocol/Internet Protocol – im Internet weit verbreiteter Netzwerkprotokollsatz, der die Kommunikation zwischen verbundenen Computernetzwerken mit verschiedenen Hardware-Architekturen und Betriebssystemen ermöglicht. TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

Trojaner

Ein bösartiges Programm, das sich als eine legitime Anwendung ausgibt. Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können ebenso schädlich sein. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Viren zu befreien, stattdessen aber den Rechner infiziert.

Der Begriff entstammt einer Geschichte in Homers "Ilias", in der die Griechen ihren Feinden, den Trojanern, angeblich als Sühnegabe ein riesiges hölzernes Pferd schenkten. Aber nachdem die Trojaner das Pferd in die Stadt gebracht hatten, schlichen sich die im Bauch des hölzernen Pferdes versteckten Soldaten bei Nacht heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsleuten, in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Update

Eine neue Software- oder Hardwareversion, die eine ältere Version desselben Produkts ersetzt. Die Update-Installationsroutine eines Programms prüft oft, ob eine ältere Versionen auf dem Rechner installiert ist, da sonst kein Update installiert werden kann.

Bitdefender verfügt über ein eigenes Update-Modul, das die manuelle oder automatische Suche nach Updates ermöglicht.

Virus

Ein Programm oder ein Stück Code, das auf einen Rechner kopiert wird und sich allein ausführt, ohne dass es der Besitzer des Rechners will oder merkt. Die meisten Viren können sich auch selbst vervielfältigen. Alle Computerviren wurden von Menschen programmiert. Ein Virus, der sich immer wieder vervielfältigen kann, ist sehr einfach zu programmieren. Sogar ein solch einfacher Virus kann gefährlich sein, da er im Handumdrehen sämtlichen Arbeitsspeicher belegen und so das System lahmlegen kann. Noch gefährlicher sind Viren, die sich über Netzwerke selbst weiterversenden und Sicherheitssysteme umgehen.

Wurm

Ein Programm, das sich selbst kopiert und über ein Netzwerk verbreitet. Es kann sich nicht an andere Programme anhängen.